DESIGN A NEW CRYPTOSYSTEM

Md. Shamim Hossain Biswas

Publication Partner: IJSRP INC.

11/10/2019

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

DESIGN A NEW CRYPTOSYSTEM

M.S.H. Biswas Cryptosystem

Md. Shamim Hossain Biswas

Publishing Partner:
IJSRP Inc.
www.ijsrp.org

https://doi.org/10.29322/ijsrp.29.12.2019

Preface

Alhamdulillah, all praises to ALLAH (subhanahu wa ta′ala) who gives me the ability to complete this research work. I could not have finished my work if Almighty ALLAH did not make it possible.

I would like to give special thanks to Dr. Touhid Bhuiyan (Heads and Professor, Department of Software Engineering, Daffodil International University) who provided opportunity to do this research.

I am very grateful to Mr. Md. Maruf Hassan for his inspirational advices in cryptography lectures. I had motivated to cryptography by his inspiration and contented by reading cryptography.

I am very grateful to Abu Shamim Aminur Razzaque for his rigorous encouragement and good academic advocating.

I am very grateful to Mr. Md. Khaled Sohel who instructed me to find out research gaps during the decision period of my research activities.

I would like to give thanks to M. Mostafa kamal who is trainer and writer of a number of books on English language for helping me during correction time of this research.

I would like to vote of thanks to Dr. Md. Asraf Ali who gave some important instruction during this research.

I would like to extend my gratitude to my respectful supervisor Dr. Md Mostafijur Rahman. Because, he guided me to carry the work and gave me important advice whenever I was in a dilemma.

All of them have contributed to present suitable atmosphere prevailing at Daffodil International University that facilitates me to make research activities. This research would not exist without them. They have been a continual source of support and motivation (visible or invisible) and have provided me with insightful information from differing points of view. Their excellent guidance, motivation, caring, patience provided me with an excellent facilities and environment for doing this research.

I would like to express my gratitude and happiness to my parents, my beloved wife, brothers and sisters for their continued support, inspiration, patience and love. I am very grateful to my family members who supported financially to conduct study because without their financial support, love and affection, this work could not carry out. Last but not least, thanks goes to whoever has helped me either directly or indirectly in accomplishment of my research.

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

Copyright and Trademarks

I hereby declare that this research monograph becomes the property of Md. Shamim Hossain Biswas and to be placed at the worldwide database access library for future cryptographic researchers and also be available Online.

Author Biography: **Md. Shamim Hossain Biswas**

MA in English: Language, Literature, TESOL (North South University)

MSc in Software Engineering (Daffodil International University)

BSc in Computer Science & Engineering (Stamford University)

ORCID: 0000-0002-4595-1470

shamim44-165@diu.edu.bd

Cell:+8801531262445

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

LIST OF ABBREVIATIONS

ACRONYM		EXPANSION
AVISPA	:	Automated validation of Internet Security Protocols and Applications
IAIK	:	Institute for Applied Information Processing and Communications
SWIFT	:	Society for Worldwide Interbank Financial telecommunication
ASCII	:	American standard Code for Information Interchange
OEIS	:	The On-Line Encyclopedia of integer sequences
WIPR	:	Weizmann-IAIK Public-key for RFID.
RAMON	:	Rabin-Montgomery *Cryptosystem*
CID	:	Smart Card Identification Number
BAN logic	:	Burrows–Abadi–Needham logic
RFID	:	Radio Frequency Identification
H(m)	:	Collision resistant hash function
CRT	:	Chinese Remainder Theorem
Crypto	:	Encryption and Decryption
R	:	Residue or Arbitrary number
RSA	:	Rivest, Shamir and Adelman
ECC	:	Elliptic curve Cryptography
PID	:	Principal of Ideal Domain
ID_i	:	User Identification Number
crypto++	:	Cryptographic Frame work
GCD	:	Greatest Common Divisor
QNR	:	Quadratic Non Residuum
RGB	:	Read and get the bands
SDR	:	Software Defined Radio
MANET	:	Mobile Ad Hoc Network
PNT	:	prime number theorem
H. C. William	:	Hugh Cowie William
Stego-object	:	Steganography object
PU_A	:	Public key of Entity A
PRb	:	Private key of Entity B
UHF	:	Ultra High Frequency

(ID_A)	:	Identifier of Entity A
QR	:	Quadratic residue
Ad Hoc	:	For this/created
R.H.S	:	Right hand side
Rc	:	random nonce
L.H.S	:	Left hand side
H- Rabin	:	Hayder-Rabin
SK	:	Session Key
US	:	United State
e_k	:	Encryption
d_k	:	Decryption
Vierergruppe	:	Four Group
PW	:	Password
Mod	:	Modulus
Mod	:	Modulo

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

LIST OF SYMBOLS

SYMBOLS		SYMBOLIC MEANINGS
$\omega(n)$	:	Number of distinct prime divisors of n
HAC	:	Handbook of Applied Cryptograph
$\mathcal{G}2$	:	Mathematical bold script capital G
$H\ (m)$	:	Collision resistant hash function
$\oplus$	:	O-plus or exclusive or operation
$\otimes$	:	N-Ary circular times operator
$((x))$	:	Sawtooth function of period 1.
$\Omega(n)$	:	Number of prime factors of n,
$\equiv$	:	Identical to or congruent to
$x = \sum_{i=1}^{k} aiMiNi$	:	Chinese Remainder formula
$\subsetneq$	:	A subset of nor a equal to
$\mathfrak{R}$	:	Bold Fracture Capital R
$\omega(n)$	:	Prime Omega Function
φ	:	Euler's totient function
$\left[\frac{\alpha}{\pi}\right]_4$	:	Quartic residuosity
$\nexists$	:	There does not exist
$\mathbb{R}$	:	Rational number set
$\doteq$	:	approaches to limit
$\left(\frac{a}{N}\right)$	:	Legendre Symbol
$a\ +\ bi$	:	Gaussian Integers
∂	:	Partial differential
ς	:	Greek letter Sigma
$\nmid$	:	Doves not divide
μ(n	:	Mobius Function
$Q(\zeta_{2^\ell})$.	:	cyclotomic fields
$(H,*)$	:	Homomorphism
λ(n)	:	Liouville function,
$\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$	:	Jacobi Symbol
$\Im$	:	Black capital I
$\mathbb{F}$	:	Finite number
©	:	Copyright Sign

$\mathbb{G}$	:	Set of generator
$D(a,b,c) = \sum_{c \bmod n=1}^{n-1} \left(\left(\frac{ac}{n}\right)\right)\left(\left(\frac{bc}{n}\right)\right)$	:	Dedekind Sum
$\|\|$	:	Concatenation
g^t	:	Primitive Root
$\equiv$	:	Corresponds to
$\mathbb{F}$	:	Finite number
ω	:	Small Omega
$a\|p$	:	A dived by p
(G,*)	:	Set of group
$=:$	:	Equal colon
$\mathbb{Q}$	:	Quotient set
$\triangleq$	:	Ring equal to
E	:	There exist
$\mathbb{Z}$	:	Integer set
$\mathbb{F}$	:	Finite set
[ ]	:	Reciprocity
Σ	:	Summation
$\sqcup$	:	Sideways U
$\in$	:	Element of
$::$	:	Proportion
$\mathcal{G}$	:	Capital G
ζ	:	small zeta
$\therefore$	:	Therefore
$\forall$	:	For All

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

ABSTRACT

The cryptography is the art of protecting information by transforming encryption into unreadable format called cipher text. Only those who possess a secret key can decipher the message into plaintext. Either single or more cryptographic primitives are often used to develop a more complex algorithm which is called cryptosystem. Michael O. Rabin Cryptosystem can generate same ciphertext form different plaintext as well as multiple plaintext from single cyphertext. There are a number of techniques to reveal original plaintext, but none of them can separate similar cyphertext against each plaintext generated from modular reduction arithmetic. Another problem is forgery attack on Rabin signcryption algorithm and private key derivation. To solve those issues, a new cryptosystem has been designed which can efficiently separate similar ciphertext against each plaintext by removing all of the problem of Rabin cryptosystem identified in problem statements. The proposed cryptosystem comprises five algorithms: Key generation, Encryption, Decryption, Signature generation and Signature verification algorithm. To authenticate message, the syncryption algorithm has been designed. The proposed cryptosystem construction based on quadratic residue, quadratic quotient, floor function and absolute value counting, Diffie-Hellman key exchange protocol, concept of Michael O. Rabin signature algorithm, and probability theorem. The advantage of proposed crypto intensive technique is intended receiver gets only one plain value distinguishing the ciphertext against the plaintext by verifying signature of sender. Another advantage is that the sender generate signature using encrypted text and intended receiver can retrieve plaintext from signature through signature verification system. The proposed crypto technique requires less time complexity and probably secure against man-in-the-middle attack, chosen plaintext, cyphertext attack and modular squaring attack. The newly designed techniques uses random padding system including additional quotient and residuum. In terms of signature, Rabin signature is pair but proposed cryptosystem uses 4-tuple signature system.

Keywords

Cryptosystem, key distribution protocol, Extended Euclidean Algorithm, Chinese Remainder Theorem, Legendre Symbol, Congruence, ASCII- Code, Quadratic reciprocity, Jacobi Symbol, Dedekind sum. Group isomorphism, Cipher, Biswas cryptosystem.

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

CHAPTER 1

INTRODUCTION

1.1 Background

The cryptography is the art of practice and study of techniques for secure communication in the presence of third parties called adversaries. It is a branch of cryptology. Cryptology is the scientific study of cryptography, cryptanalysis and steganography. The cryptography is the art of protecting valuable information by transforming encrypted data into unreadable format that is called cipher text. Only those who possess a secret key can decipher the message into readable format. Encrypted message can be broken by cryptanalysis that is called code breaking, although modern encryption techniques are virtually unbreakable. Cryptography is used to secure data in transmission, data storage and user authentication. Cryptography involves creating codes that allow information to be kept secret, cryptography converts data into an unreadable format so that an unauthorized user unable to decode while transmission. It replaces the handwritten signature to digital signature. Digital signatures are used to credit card authentication. Due to having the large number of commercial transactions over the internet, the cryptography is the main key in ensuring the security of the transmissions. In general, cryptography plays an important role for data confidentiality, data integrity, user authentication and non-repudiation. The cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. More complex cryptosystems include electronic cash systems, signcryption system, etc. A sophisticated cryptosystem can be derived from a combination of several cryptographic primitives. Cryptosystems are sometimes called cryptographic protocol. In physical world, handwritten signatures are used to bind the signatory to the message analogously in digital world, the signcryption system is used to bind signatory to the digital message. Actually the message signing binds the identity of the message. It ensures the data integrity, message authentication and non-repudiation. There are different types of cryptosystems: Asymmetric key cryptosystem, Symmetric key cryptosystem, Hybrid cryptosystem, Knapsack cryptosystem, etc. Michael O. Rabin cryptosystem was one of the first asymmetric cryptosystem in the field of public key Cryptography. Security of Rabin encryption mechanism relies on prime integer factorization. (Rabin, 1976, 1979) proposed a public key cryptosystem and signature scheme. Together with encryption, decryption and signature schemes are called Michael O. Rabin cryptosystem. A large number of surveys were done on Michael O. Rabin cryptosystem to find out its efficiency and devise a new method for real life application. It has huge theoretical significance in cryptography. There are two light weight public key cryptosystems: Elliptic Curve Cryptosystem (ECC) and Rabin cryptosystem. Two public key protocol based on Rabin cryptosystem are used in implementation Ultra High Frequency (UHF RFID) and Radio Frequency Identification Reader (RFID) (Saxl.et.al. 2019). A slightly modified version of Rabin Cryptosystem (RAMON

cryptosystem) was used in implementation of UHF RFID and WIPR (Sensors). The Rabin cryptosystem is used in passive radio frequency identification by slightly modification. The encryption mechanism used to quadratic residue to produce cipher text and Decryption was accomplished by Computing two square root, Bezout's coefficient using extended Euclidean algorithm and combining them with Chinese Remainder theorem. It was quite similar to RSA and ElGamal cryptosystems, Michael O. Rabin cryptosystem considered in ring under addition and multiplication modulo composite integer.

In cryptography, Michael O. Rabin cryptosystem produces four decryption results of which one is correct and other three are pseudo results. However, those disadvantages turned into advantage in steganography on the other hand. Three illusion message brought benefit to steganography applications. Although, in cryptographic application, those three false results considered a weak point in Rabin cryptosystem due to the size problem. The disadvantage of Rabin Cryptosystem turned into advantage in steganography field which would be used not only constructing hiding map but also authenticated mechanism which guides the hiding process. The decryption algorithm will give four message of which one is secret message and the rest of three are illusion messages with a different length that will construct the map of graphical data.

1.2 Motivation of the research

With the growth of the Internet, encryption came into much wider use to protect credit card and other online transactional information. Only in the past decade, encryption has been widely used for ordinary communications and stored data because the number of genius hacking techniques is noticeably increasing day by day. Robbery in Bangladesh bank, for example, took place on (Editor, 2016), when thirty five fraudulent instructions were issued by security hacker via the SWIFT (Society for Worldwide Interbank Financial Telecommunication) inter-bank messaging system to illegally transfer to US. The attack resulted in the theft of $101 million of which $81 million remain missing. If we have had crypto-intensive technology, this type hacking robbery could not have taken place. This is not only Bangladeshi cyberspace problem but also worldwide developing countries' cyber problem, although, the challenge of designing practical and secure encryption system is magnified by the fact that the encryption algorithms and protocols are notoriously fragile. Cryptosystem is the most effective way to achieve data security. So thinking about aforesaid security and privacy issues in cyberspace, I devoted myself to continue study on Cryptography to ensure confidentiality and security in communication. In fact, security and privacy issues are entirely two different beasts in information communication system. Since cryptography is a domain of computer and information security which is an evolving discipline that involves the study of technology, strategy, policies and standards regarding the security of and operations in cyberspace, it refers to secure information and communication techniques derived from mathematical concepts and set of rule based calculations called algorithms which transforms message in a ways that are hard to decipher. For those aforesaid reasons, I have been motivated in applied cryptography subject which is a branch of cryptology.

1.3 Problem Statement (Research Gaps)

To find out research gap is mandatory to do research and for that reasons literature reviews are necessary. Research gap analysis is also conducted through literature review in order to see how the proposed research methodology would fill in the gap in the research area. Michael O. Rabin Cryptosystem was not widely used because of having some computational error during encryption and decryption produced by modular arithmetic but its theoretical significance is widespread. However, RAMON cryptosystem is used in RFID reader. It was implemented based on Rabin cryptosystem. On the other hand, Rabin signature is vulnerable in forgery attack. One of the main disadvantages is to generate four results during decryption and extra effort needed to sort the right one out of four possibilities. Recently, many rigorous articles about Rabin cryptosystem have been published in different journals and conferences by researchers. A number of problem and ambiguity was noticed in Michael O. Rabin Cryptosystem during literature review and formulated in following steps.

Issue-1: Rabin Encryption and Decryption system generates same cipher text from different plaintext for example, two random private key P=7, Q=11, public key $N=P*Q=7*11=77$. M = {13, 20, 57, 64} four plaintext produce same cypher(c) = M^2 mod 77=15 and the same way it produces multiple plaintext from single cipher text during decryption. There is no algorithm to identify similar quadratic residue generated from distinct input in Michael O. Rabin Cryptosystem, the following example may be efficient for cryptographic readers.

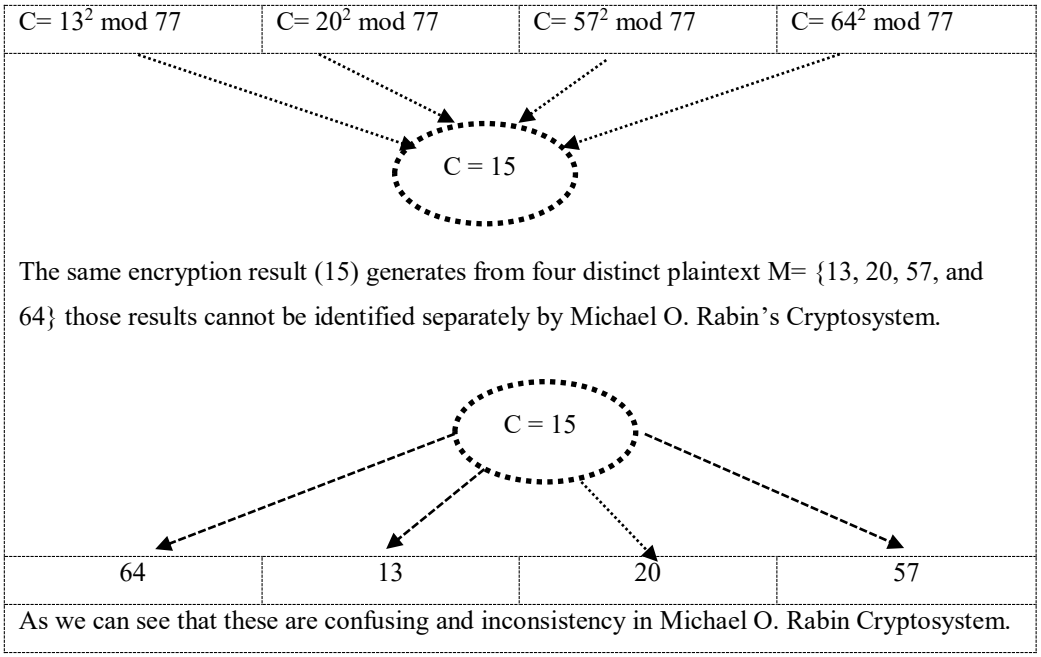


Figure 1.1: Research gaps in Michael O. Rabin Cryptosystem

Issue-2: Private Key can be obtained through combination of two modular exponentiations, Chinese Remainder Theorem and Extended Euclidean algorithm. For example, apply GCD (|r-s|, N) where r and s are two roots. For example, GCD (57-13, 77) = GCD (44, 77) =11 which is Q and P=N/Q=77/11=7.

Issue-3: The decryption of Rabin's Cryptosystem is non deterministic.

Issue-4: Rabin's signature scheme is vulnerable to forgery attacks. It is relatively easy to compute S^2 modulo N by choosing any message m' and compute multiplicative inverse of m' (hash value of m) and then calculate $U' = S^2 * m'^{-1} \, mod \, N$ and forge the signature as (m'^{-1}, U', s) without knowing the factorization of N. Assuming two Blum primes are $p = 7, q = 11.$ Public key $N = p.q = 77, m = 20, m' = m^2 = 20^2 \bmod 77 = 15$ is hash value. Taking two values $U = 25$ and $x = 12$ arbitrarily for which the equation $12^2 \bmod 77 = (15 * 25) \bmod 77$ is true. Hence, the signature $\{15, 25 \text{ and } 12\}$ and the forgery signature $\{36, 25 \text{ and } 12\}$, where 36 is multiplicative inverse of 15. Where $U' = x^2.m'^{-1} \bmod N = 12^2.36 \bmod 77 = 25$ where Multiplicative inverse $(m'^{-1}) = 36$. The forgery attacker forges the signature as (m'^{-1}, U', x). Since the $U = U'$, $s = x^2 \bmod N$ and m'^{-1} the multiplicative inverse of m'.So the signature is valid mathematically and forgery attacker become successful to achieve signature.

1.4 Research Questions

The research questions have already been mentioned in problem statements, even after presenting research questions more precisely for entire future cryptographic reader, the following question may be ideal for them.

- ✓ How one can separate similar quadratic residue generated from different input in Michael O. Rabin cryptosystem?

1.5 Research Objectives

- To solve similar quadratic residue identification problem of Rabin cryptosystem.
- To design a new cryptosystem.
- To solve modular crashing attack on Michael O. Rabin Cryptosystem.
- To counteract forgery attack on Rabin's syncryption algorithm.

1.6 Research Scope

The research scope is limited to design a new cryptosystem to overcome the constraints of Michael O. Rabin Cryptosystem. The process of designing technique is as follows.

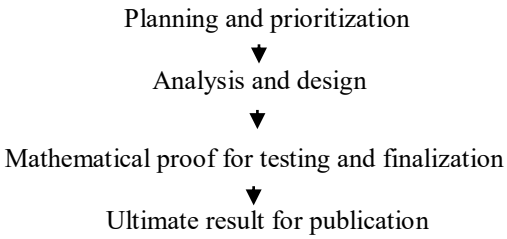


Figure1.2: Research scope

In the planning and prioritizing phase, Research gaps finding (mission statement) and decision taking (selection of vision statement) are main concern of research. Analyzing and design phase ensure designing of cryptosystem in particular, how desired problem's solution will be implemented using different methodology. Mathematical experiment for testing and finalization ensures whether proposed techniques result in correct answer?

1.7 Thesis Organization

The road map of this research has been organized in the following ways.

Chapter 1 briefly introduced the research background and some primary knowledge about Michael O. Rabin Cryptosystem. The problem statements (research gaps), research objective and research scope are introduced in this chapter. The rest of the research is organized as follows.

Chapter 2 consists of literature review and preliminaries related to Michael O. Rabin Cryptosystem.

Chapter 3 describes research methodology which indicates how I performed my research activities.

Chapter 4 presents the author contribution and detail descriptions of research outcome has been given. A comparison between newly designed cryptosystem and Michael O. Rabin cryptosystem has also been demonstrated.

Finally, Chapter 5 gives conclusion and future work for potential innovative reader.

CHAPTER 2

LITERATURE REVIEW

2. 1 Preliminaries

The Euclidean algorithm is used to finds the greatest common divisor (GCD) of two numbers a, b ∈ N. It essential for Michael O. Rabin cryptosystem. The algorithm is as follows.

- First initialize the $r_0 = a, r_1 = b$
- Now compute the following sequence of steps:

  $r_0 = q_1 * r_1 + r_2,$

  $r_1 = q_2 * r_2 + r_3,$

  $r_{n-3} = q_{n-2} * r_{n-2} + r_{n-1}$

  $r = q_{n-1} * r_{n-1} + r_n$ Continue this process until there is a step for

  which $r_n = 0$ while $r_{n-1} \neq 0$.

- The greatest common divisor is equal to r_{n-1}.

The extension of above algorithm is called extended Euclidean algorithm which is useful in the finite field and in encryption algorithm. The Extended Euclidean algorithm not only calculates the gcd but also two additional integers x and y that satisfy the equation. $a * x + b * y = gcd(a, b) = d$. It is clearly appears opposite sign of x and y after examining algorithm. The extended Euclidean algorithm (Table 2.1) which determines x, y, d from given a and b where a ≥ b ≥ 0. (Stallings, 2016).

Table 2.1: The extended Euclidean algorithm

Initial		Extension	
Calculates	division	$x_{-1} = 1,\ y_{-1} = 0$	$a = a * x_{-1} + b * y_{-1}$
$r_{-1} = a,\ r_0 = b$		$x_0 = 0,\ y_0 = 1$	$b = a * x_0 + b * y_0$
$r_1 = a \bmod b$ $q_1 = \left\lfloor \frac{a}{b} \right\rfloor$	$a = b * q_1 + r_1$	$x_1 = x_{-1} - q_1 * x_0 = 1$ $y_1 = y_{-1} - q_1 * y_0 = -q_1$	$r_1 = a * x_1 + b * y_1$
$r_2 = b \bmod r_1$ $q_1 = \left\lfloor \frac{b}{r_1} \right\rfloor$	$b = r_1 * q_2 + r_2$	$x_2 = x_0 - q_2 * x_1$ $y_2 = y_0 - q_2 * y_1$	$r_2 = a * x_2 + b * y_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \left\lfloor \frac{r_1}{r_2} \right\rfloor$	$r_1 = r_2 q_3 + r_3$	$x_3 = x_1 - q_3 * x_2$ $y_3 = y_1 - q_3 * y_2$	$r_3 = a * x_3 + b * y_3$
: :	: :	: :	: :
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor$	$r_{n-2} = q_n * r_{n-1} + r_n$	$x_n = x_{n-2} - q_n * x_{n-1}$ $y_n = y_{n-2} - q_n * y_{n-1}$	$r_n = a * x_n + b * y_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$	$r_{n-1} = q_{n+1} * r_{n+0}$		$d = gcd(a, b) = r_n$ $x = x_n, y = y_n$

Bezout′s Identity (Bezout, 1779) is a GCD related theorem which is valid for every principal ideal domain. A pair of Bezout′s coefficients can be computed by the extended Euclidean Algorithm. Modular arithmetic deals with whole numbers where numbers are replaced by their remainders after division by a fixed number in a modular arithmetic. Modular division is defined when modular inverse of the divisor exists. There are number of rules in modular arithmetic which is efficient in scientific experiment. Modular arithmetic is a system of arithmetic for integers, where values reset to zero and begin to increase again, after reaching a certain predefined value, called the modulus (modulo). Modular arithmetic is widely used in computer science and cryptography. The clear description of modular arithmetic can be found in (Gauss, et.al., 1965). The Chinese remainder theorem (CRT) is essential for Michael O. Rabin cryptosystem. The CRT asserts that composite number N is pairwise coprime for that the system of congruence $x \equiv a_1 \pmod{N_1}$, $x \equiv a_2 \pmod{N_2}$ where N_1, N_2 are coprime. Bezout's identity asserts the existence of two integers m_1 and m_2 such that $m_1N_1 + m_2N_2 = 1$. The formula of CRT is as follows.

$$\sum_{i=1}^{k} aiMiNi \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots . Equ. (1)$$

The details about *Equ.(1)* can be found in (*Katz,et.al.,1998*).

The polynomial is an expression consisting of variables and coefficient. It involves addition, subtraction, multiplication operations and non-negative integer exponential variables. The novel polynomial equation is as follows

$a_n\, x_n + a_{n-1}x^{n-1} \ldots\ldots a_2x^2 + a_1x^1 + a_0x^0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots Equ.(2)$

Equ.(2) can be expressed more precisely by using summation notation is as follows.

$$\sum_{k=0}^{n} a_k x^k \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots Equ.(3)$$

For more details about *Equ.(3),* see (*Manuel,et.al,2006*). The Legendary symbol is a number theoretic function $\left(\frac{a}{p}\right)$ which is defined to be equal to ±1 depending on whether α remains quadratic residue modulo p. The definition of Legendre symbol is as follows.

$$\left(\frac{a}{p}\right) = a|p = \begin{cases} 0 & if\ \ p|a \\ 1 & if\ a\ is\ a\ quadratic\ residue\ modulo\ p \\ -1 & if\ a\ is\ a\ quadratic\ nonresidue\ modulo\ p \end{cases} \quad \ldots\ldots\ldots Equ.(4)$$

If p is an odd prime, the Jacobi symbol reduces to the Legendre symbol. The Legendre symbols obey the following identity

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots Equ.(5)$$

In general, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}\ (mod\ p)$ if p is an odd prime. For more details, see (Jones, et.al., 1998). The ASCII characters are associated to an integer value for each symbol, letters, digits, punctuation marks, special characters and control characters. It is essential for communication system. The ASCII table (Karen, et.al. 2012) is presented in "Appendix A". In mathematics and computer science, the floor function takes input x and gives output as an integer which less than or equal to x. The details about this can be found in (Knuth, et.al., 1988). Mobius function was introduce by the German mathematician August Ferdinand Mobius in 1832. It has many application in computer Science. For any positive integer n, define μ(n) as the sum of the primitive n-th roots of unity. It has values in $\{-1, 0, and\ 1\}$ depending on the factorization of n into prime factors:

- $\mu(n) = 1$ If n is a square-free positive integer with an even number of prime factors.
- $\mu(n) = -1$ If n is a square-free positive integer with an odd number of prime factors.
- $\mu(n) = 0$ If n has a exponential prime factor. For example, the Table 2.2 shows Mobius functionality is as follows.

Table 2.2: Mobius function interpretation for 10 positive numbers.

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	1	−1	0	−1	-1	−1	0	0	-1

The Mobius function can alternatively be represented as $\mu(n) = \delta_{\omega(n)}^{\Omega(n)}$ where δ is the Kronecker delta, λ(n) is the Liouville function, $\omega(n)$ is the number of distinct prime divisors of *n*, and $\Omega(n)$ is the number of prime factors of *n*, counted with multiplicity.

Table 2.3: shows an alternative form of Mobius interpretation for 10 positive numbers.

n	1	2	3	4	5	6	7	8	9	10
$\mu(n) = (-1)^{\Omega(number\ of\ prime\ factor)}$	1	-1	−1	0	−1	1	−1	0	0	1

The Mobius function can be expressed by $\sum_{d|n} \mu(d) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots . Equ\ (6)$

For more details about $Equ\ (6)$, see (Hardy,et.al.,1990, *Klimov, 2001*). The radio frequency identification (RFID) devices have been recently introduced in several applications and services as National Identification Cards, Passports, credit cards, etc. A passive radio frequency identification (*RFID*) reader for two dimensional localization of tagged objects in the ultra-high frequency. A software defined radio (SDR) system for measurements of minimum activation power and backscatter power of ultra-high frequency reader (UHF RFID). A device conducting RFID eavesdropping using software defined radio platform (SDRP). A classical RF attacks can be made on long range transmission protocols, however we extend the standard RF attacks to cover RFID communication protocols. For more clarification, see (Alex,et.al., 2014).The Jacobi symbol $\left(\frac{a}{N}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right)$ is the quadratic residuosity, it was used to distinguish the roots in the Rabin cryptosystem, when $p \equiv q \equiv 3\ mod\ 4$. For primes congruent to 1 modulo 4, The Legendre symbols cannot distinguish numbers of opposite sign, therefore quadratic residuosity is no longer sufficient to identify the roots. Higher power residue symbols could be efficient for desired job, but unfortunately their use is not straight forward and analogous reciprocity laws or multiplicative properties are not always at hand. Higher power residues have been used in some generalizations of the Rabin scheme working in residue rings modulo non-prime ideals of algebraic number fields. For instance, residue rings in Eisenstein or Gauss fields were considered and Rabin-like schemes based on encryption rules involving powers of the message higher than 2 were introduced. This approach does not address the problem of separating the roots of a quadratic equation in the classic Rabin scheme. Therefore, it is necessary to look at different kinds of higher order residuosity which should allow a reciprocity law, a finite group which does not reveal any information allowing the factorization of N. An idea is to multiply the exponent and consider the function which would identify message among the roots of unity in Z_{*N}. This idea would be to make these roots publicly available and label them so that the sender of the message can tell which of them corresponds to the message actually sent. But it is necessary to masking by multiplying odd number in order to hide the factors N and most importantly we would find the square roots among the root of unity. The multiplicative group Z_{*N} which is direct product of two cyclic group $\mathfrak{C}_{p-1}\ and\ \mathfrak{C}_{q-1}$, can also be viewed as the direct product of two abelian subgroups, namely $\mathcal{G}2$ and a group of odd order that is

$Z_{*N} = (\mathfrak{e}_2^k \times \mathfrak{e}_2^h) \times (\mathfrak{e}_{2fp+1}^k \times \mathfrak{e}_{2fq+1}^h)$. Therefore, every element α of Z_{*N} can be written as a product. Vierergruppe is a group with four elements in which each element is self-inverse. It is non cyclic group. It is however an abelian group and isomorphic to the dihedral group of order 4. This group consists of three elements and an identity element. For example, four roots can be presented as $V_4 = \{1, -1, \psi, \psi\}$. This theoretical phenomenon would be clearer by following tree representation of correct root identification.

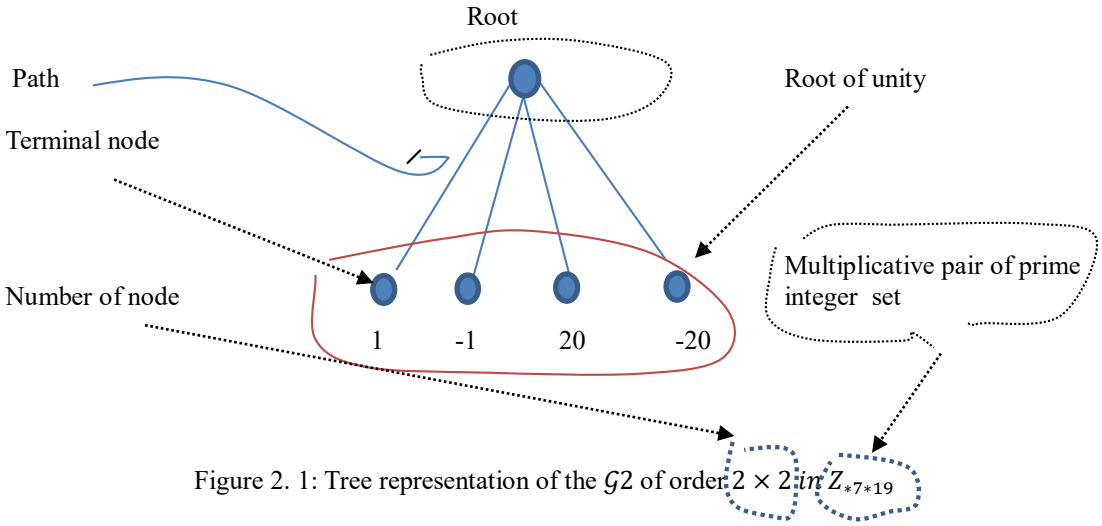


Figure 2. 1: Tree representation of the $\mathcal{G}2$ of order 2×2 *in* Z_{*7*19}

For more details, seee (Takagi, et.al., 1997, Frohlich, et.al., 1994, Ireland, et.al., 1998, Lemmermeyer, 2000). In group theory, two groups are said to be isomorphic if there exists a bijective homomorphism. Group isomorphism theorem known as the homomorphism theorem. In this research activities, a practical method have been described in context of Michael O. Rabin cryptosystem working with any pair of primes that can have acceptable complexity, although it requires a one-way function that might be weaker than factoring. The public key consists of the two function. At the encryption stage both are evaluated at the same argument, the message m and the minimum information necessary to distinguish their values is delivered together with the encrypted message. The decryption operations are obvious. The true limitation of this scheme is that function must be a one-way function, otherwise two square roots that allow us to factor N can be recovered as in the residuosity subsection. For more details, see (Wikipedia). The Dedekind sums were introduced by Richard Dedekind. It is denoted by D (a, b, c) and the classical Dedekind sum was denoted by.

$$D(a,b,c) = \sum_{c \bmod n=1}^{n-1} \left(\left(\frac{ac}{n}\right)\right)\left(\left(\frac{bc}{n}\right)\right) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Equ.(7)$$

The terms on the right of *Equ.(7)* being the Dedekind sum. For the case a=1, one often writes $S(b,c) = D(1,b;c)$. Let C, N be relatively prime and N ≥ 1, then we set the methods of computation based only on the residue theorem from complex analysis. In mathematics, Dedekind sum are certain sums of products of a sawtooth function, and are given by a function *D* of three integer variables. Dedekind introduced them to express the functional equation of the Dedekind eta function. The well-known classical Dedekind sum is as follows.

$$S(b,c) = \sum_{c \bmod n=1}^{n-1} \left(\left(\frac{c}{n}\right)\right)\left(\left(\frac{bc}{n}\right)\right) \dots\dots\dots\dots Equ.(8)$$ positive integers or coprime

and the sawtooth function is as follows.

$$((x)) := \begin{cases} (x) - \lfloor x \rfloor - \frac{1}{2} & if\ x\ is\ not\ an\ integer. \\ 0 & otherwise. \end{cases} \dots\dots\dots\dots Equ.(9)$$

The symbol ((x)), denotes the well-known Sawtooth function of period 1.

The Dedekind sum satisfies different properties but here only few of them has been shown because of a number of author used Dedekind sum to solve Michael O. Rabin cryptosystem which will be clarified at the end stage of literature review,

$c_1 = c_2 \bmod n \Rightarrow S(c_1,n) = S(c_2,n)$.....*Equ.(10)*

$S(-c, n) = -S(c, n)$.....*Equ.(11)*

$S(c, n) + S(n, c) = -\frac{1}{4} + \frac{1}{12}\left(\frac{c}{n} + \frac{1}{cn} + \frac{n}{c}\right)$ .....*Equ (12)*

Equ.(10) to Equ.(12) known as the reciprocity theorem for Dedekind sums

$12n\,S(c,n) = n + 1 - 2\left(\frac{c}{n}\right) mod\ 8$ .....*Equ (13)*

Equ.(13) for odd number n, this property connecting Dedekind sums and Jacobi symbols. The first three properties allow us to compute a Dedekind sum by a method that mimics the Euclidean algorithm and has the same efficiency. In the sequel, we need the following Lemma, If n =1 mod 4, for any c relatively prime with n, the denominator of S(c, n) is odd. In the definition of S(c, n) we can limit the summation to $n-1$ because $\left(\left(\frac{n}{n}\right)\right) = 0$, furthermore, from the identity $((-x)) = -((x))$ it follows that

$\sum_{b=1}^{n-1}\left(\left(\frac{bc}{n}\right)\right) = 0$ for every integer c, so we may write the following formula

$$S(c,n)=\sum_{b=1}^{n-1}\left(\frac{b}{n}-\frac{1}{2}\right)\left(\frac{bc}{n}-\left\lfloor\frac{bc}{n}\right\rfloor-\frac{1}{2}\right)=\sum_{b=1}^{n-1}\frac{b}{n}\left(\frac{bc}{n}-\left\lfloor\frac{bc}{n}\right\rfloor-\frac{1}{2}\right)\ldots\ldots Equ(14)$$

Since $\left(\left(\frac{bc}{n}\right)\right)$ is never 0, because b < n and c is relatively prime with n by hypothesis. *Equ(14*) can be split into two further summations is as follows.

$$\sum_{b=1}^{n-1}\frac{b}{n}\left(\frac{bc}{n}-\left\lfloor\frac{bc}{n}\right\rfloor\right)\ldots\ldots\ldots\ldots Equ(15)\text{ and its denominator patently odd}$$

$$-\frac{1}{2}\sum_{b=1}^{n-1}\frac{b}{n}=-\frac{n-1}{4}\ldots\ldots Equ.(16)$$

For more details. See (Choi, et.al., 2018, Grosswald, 2009). The Dirichlet theorem was invented by John Peter Gustav who was a German mathematician who contributed to number theory, Fourier series and mathematical analysis. In number theory, Direclet's theorem is called Direclet prime number theorem which states that for any two positive coprime integers a and d. There are infinitely many primes formation. The lists several arithmetic progression with infinitely many primes are shown in "Appendix B" which is collected from OEIS number sequence. A prime number is a natural number greater than 1 that cannot be formed by multiplying two smaller natural numbers. Stronger forms of Dirichlet′s theorem state that any arithmetic progression the sum of the reciprocals of the prime numbers in the progression diverges and different such arithmetic progressions with the same modulus have approximately the same proportions of primes. The strong form of Dirichlet's theorem implies a divergent series that is an infinite series. It is not convergent. It means that the infinite sequence of the partial sum series does not have a finite limit. For more details see (Vari, 2014). The forking lemma is any number related lemma in cryptographic research. This concept was first used by David Pointcheval and Jacques Stern in "Security proofs for signature schemes," published at Eurocrypt in 1996. The forking lemma is specified in terms of an adversary that attacks a digital signature scheme instantiated in the random oracle model. They show that if an adversary can forge a signature with non-negligible probability, there is a non-negligible probability that the same adversary with the same random tape can create a second forgery in an attack with a different random oracle. The forking lemma was later generalized by Milir Bellare and Gregory Neven. The forking lemma has been used to prove the security of a variety of digital signature schemes and other random-oracle based cryptographic constructions. The forking lemma is actually helping theorem which meaning anything is received, such as a gift, profit, or a bribe, Lemma's sole purpose to help in proving a theorem or your creative mathematical statements. For many signature schemes, having two signatures using the same randomness for two different hash values allows recovery of the private key. This is used in many security proofs by showing that an adversary that forges a valid signature can be coerced through replaying into producing two signatures of this form. As a consequence, a forgeries can be twisted into a key recovery attack. The technical question is how can we make sure that the forger is going to comply to our expectations and really forge two signatures for the same randomness. Indeed, in general, nothing

forces the adversary to use its randomness in a simple way. In particular, giving him the same coins and forcing changes the messages is not going to achieve the desired goal, because the adversary is allowed to mix the messages themselves into the randomness used for signing. The key idea is to restart the adversary with the same randomness, let it run without change until it generates the message M_0 that was signed in the first run together with its randomness and then force a change on the rest of the run. At this point, in a practical setting, we could imagine using a fault attack on the hash function. However, in a theoretical model, the change is achieved by changing the responses of the random oracle that models the hash function on the first query that involves M_0 and all subsequent queries. When we do that, we already know the behavior of the adversary until M_0 is generated and hope that it will forge again on M_0 with the same randomness but a different hash value. This is where the forking lemma comes into play. It is a technical lemma that analyzes the behavior of an adversary that receives some random values and outputs a pair of values. The result of the forking lemma is that the probability of getting two related runs with the same value. More precisely, the forking lemma makes it possible to give two different random signatures of the same message, to solve some underlying hard problem. A nice proof was given by Bellare and Neven is not too hard to follow. For more details about forking lemma, see (Bellare,et.al., 2006) . The Liouville function denoted by λ(n) and named after Joseph Liouville who was a French mathematician. It is an important function in number theory and cryptography. If n is a positive integer, λ(n) is defined as $\lambda(n) = (-1)^{\Omega(n)}$ where Ω(n) is the number of prime factors of n and counted with multiplicity.

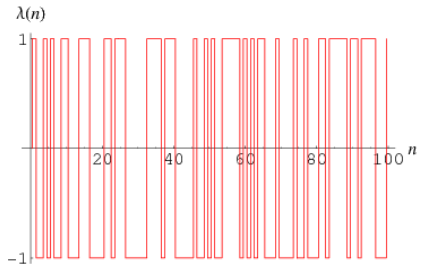


Figure 2.2: Liouville function $\lambda(n) = (-1)^{\Omega(n)}$

LiouvilleLambda(n) gives the $\lambda(n) = \mu(n) = \mu^2(n)(-1)^{\Omega(n)}$ where λ is completely multiplicative since Ω(n) is completely additive, $i.e.: \Omega(ab) = \Omega(a) + \Omega(b)$. The number 1 has no prime factors, so Ω(1) = 0 and therefore λ(1) = 1. For example, $\text{LiouvilleLambda}(20) = -1$. For the details about figure 2.2, have a look (*Peter,et.al., 2013,* Drane,et.al., 2012). The Sawtooth shaped like the teeth of a saw with alternate steep and gentle slopes. It uses for signal design and wireless communication. The convention of sawtooth wave ramps upward and then sharply drops. In the reverse saw-tooth wave, the wave ramps downward and then sharply rise. The following figure is represented to clarify the sawtooth function.

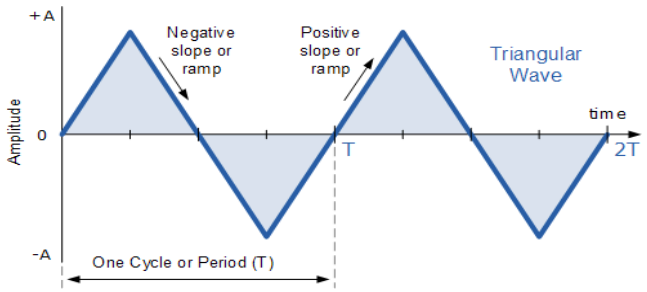


Figure 2.3: A general form of sawtooth function for Dedekind Sum

It is considered for an asymmetric triangle wave. The sawtooth waves are used for music. But in cryptography, we are just concern about general idea of sawtooth function which was used in Dedekind Sum, because real message can be retrieved using one of the properties of Dedekind sum. Rabin cryptosystem can be implemented by Dedekind sum. The product of sawtooth function is used in Dedekind sum. For more details, have a look (Rademacher, et. al., 1972).

2.2 Michael O. Rabin Cryptosystem

Michael O. Rabin cryptosystem is an asymmetric cryptographic technique. The following encryption and decryption algorithm is enlisted from (Menzes, et.al., 1997). It uses 4k+3 prime formation where K=0……N-1. There are different variant of Rabin cipher which has illustrated bellow.

2.2.1 Cipher Variant-1

`Algorithm for key generation:`

Each entity creates a public key and a corresponding private key. The entity A should do the following:

- Generate two large random and distinct primes p and q, each roughly the same size.
- Compute $n = p * q$.
- A's public key is n; A's private key is (p, q).

`Algorithm for Encryption:`

B encrypts a message m for A, B should obtain A's authentic public key n. then it represents the message as an integer m in the range of {0,1…. n− 1}. It computes c = m^2 modulo n and sends the ciphertext (c) to A.

`Algorithm for Decryption:`

An entity A finds the four square roots m_1, m_2, m_3 and m_4 of c modulo n. the sending message was either m_1, m_2, m_3 or m_4. A decides which one of them is desired plaintext by ascertaining replicated bits. The computation steps are as follows.

Step-1: Use the extended Euclidean algorithm to find integers Y_p and Y_q satisfying $p.Y_p + q.Y_q = 1$.

Step-2: Compute $M_p = c^{\frac{(p+1)}{4}} \ mod\ p$.

Step-3: Compute $M_q = c^{\frac{(q+1)}{4}} \ mod\ q$.

Step-4: Compute $x = (Y_p * p * M_q + Y_q * q * M_p)\ mod\ n$.

Step-5: Compute $y = (Y_p * p * M_q - Y_q * q * M_p)\ mod\ n$.

The four square roots are $x, -x, y\ and\ -y\ (modulo\ n)$.

`A workout example:` The communication between two parties start with key generation: for example, Entity A chooses the primes p = 277, q = 331, and computes n = p. q = 91687. A's public key is n = 91687, while A's private key is (p = 277, q= 331). A then declares the public key to the other party who uses the public key n to encrypt message and sends to entity A. after that the entity A decrypts message by its private key. The process of encryption and decryption is as follows.

`Encryption:` Suppose the last six bits of original messages are required to be replicated prior to encryption. In order to encrypt the 10-bit message m = 1001111001, B replicates the last six bits of m to obtain the 16-bit message m = 1001111001111001, which in decimal notation is m = 40569. B then computes $c = m^2 \bmod n = 405692 \bmod 91687 = 62111$ and sends this to A.

`Decryption:` To decrypt c, A uses aforesaid algorithm and her knowledge of the factors of n to compute the four square roots of c mod n: m_1 = 69654, m_2 = 22033, m_3 = 40569, m_4 = 51118, which in binary are m_1 = 10001000000010110, m_2 = 101011000010001, m_3 = 1001111001111001, m_4 = 1100011110101110. Since only m_3 has the required redundancy, A decrypts c to m_3 and recovers the original message (m) = 100111100

2.2.2 Cipher Variant-2

Rabin's Cryptosystem is composed of Key Setup, Encryption and Decryption. The following variant is for large prime calculation outside the prime formation of 4k+3.

Step-1: First choose random number $b \epsilon \mathbb{Z}_p$ until $b^2 - 4a$ is a quadratic non residue modulo p. i.e.,$\left(\frac{b^2-4a}{p}\right) = -1$.

By the condition on b^2-4a, *f is* irreducible. Therefore $R = \mathbb{Z}_p[x] \,/\, (f(x))$ is isomorphic to$\mathbb{F}_{p^2}$, the finite field of order p^2. Write ξ for the image of x in R. Over R we have $f(x) = (x - \xi)\,(x - \xi^p)$ so that $\xi^{p+1} = a$ in R.

Therefore $\xi^{\frac{P+1}{2}} \in \mathbb{Z}_p \subset R$.

Step-2: Let f be the polynomial $x^2 - bx + a$ in $\mathbb{Z}_p[x]$. The b is picked randomly in range (0….p). Similarly f be the polynomial $x^2 - bx + a$ in $\mathbb{Z}_q[x]$ and b is picked randomly in range (0……q). [x] is a quadratic reciprocity.

Step-3: Compute r= $(x)^{\frac{p+1}{2}}$ mod *f* and r= $(x)^{\frac{q+1}{2}}$ mod *f* using algorithm (note: r will be an integer).

Step-4: Return(r, -r) note: r= residue. r is computed using polynomial arithmetic modulo the polynomial *f*.

Note: One of several ways to compute Legendre symbol $\left(\frac{a}{p}\right)$ is as $a^{\frac{p-1}{2}}$ mod p with result p-1 replaced by -1.

A workout example:

According to congruence law. If $m^2 \equiv \alpha \, mod \, N$ where $= p * q$ =2173,

$m^2 \equiv \alpha_p \, mod \, p$, now compute $\alpha_p = 1945 \, mod \, 41 = 18$,

$m^2 \equiv \alpha_q \, mod \, q$, now compute $\alpha_q = 1945 \, mod \, 53 = 37$.

Let b=2, $(b^2 - 4a)^{\frac{P-1}{2}} \bmod 41 = (2^2 - 4 * 18)^{\frac{41-1}{2}} \bmod 41$

$$= (-68)^{20} \, mod \, 41 = ((41 * 2) - 86)^{20}$$

$$= 14^{20} = (14^5)^4 \, mod \, 41 = 40,$$

That is $p - 1$ because $41 - 1 = 40$, hence choice $b = 2$ verifies that $\left(\frac{b^2-4a}{p}\right) = -1$ and stick to it. So (p-1) replaced by -1. Now, we set polynomial for $\mathbb{Z}_p$.

f = x^2 – bx + α mod 41= x^2 – 2x + 18 mod 41= x^2 + (41– 2) x + 18 mod 41= x^2 +39x + 18 mod 41. X is a variable of a polynomial and it has not particular value. Now compute $(x)^{\frac{P+1}{2}}$ mod f that is x^{21} mod f. The binary representation of $21_{(10)} = 10101_{(2)}$

Note: Easy binary conversion.

Step-1: Divide 21 by 2 until the quotient 1 and ignore remainder.

Step-2: Set even number =0 and odd number =1.

Division =	1	2	5	10	21
Binary settings =	1	0	1	0	1

Now compute left to right binary exponentiation. X^k can rise in the following way. Just like point addition and point doubling. Means that start from x^1 and then square move to next bit (if next bit additive identify that will be added and pointer point to that one. Else if next bit is multiplicative identity that will be multiply).

Hence we can write 10101=x^2, x^4, x^5, x^{10}, x^{20}, x^{21} mod *f*

Now compute all x^k mod f under $\mathbb{Z}_{41}$,

Step-1: X^2 mod f under $\mathbb{Z}_{41}$,

$$x^2 + 39x + 18 \Big|^{\frac{1}{x^2}}_{\frac{x^2+39x+18}{-39x-18}} \text{ mod } 41$$

$$= (41 - 39)x + 41 - 18$$
$$= 2x + 23$$

Since $-39x - 18$ goes beyond the limit of $\mathbb{Z}_{41}$, so we need to turn it back to the limit.

$$-39x = (41 - 39)x = 2x \; and \; -18 = 41 - 18 = 23$$

Step-2: X^4 mod f under $\mathbb{Z}_{41} = (x^2)^2 mod\ x^2 + 39x + 18$ mod 41.

$(2x+23)^2$ mod $x^2 + 39x + 18$ under $\mathbb{Z}_{41}$.

$=4x^2 + 92x + 529$ mod $x^2 + 39x + 18$

$= 4x^2 + 10x + 37\ mod\ x^2 + 39x + 18$

$$x^2 + 39x + 18 \Big|^{\frac{4}{4x^2+10x+37}}_{\frac{4x^2+156x+72}{-146x-35}} \text{ mod } 41$$

$$= ((41 * 4) - 146)x + 41 - 35$$

$$= 18x + 6$$

Hence $x^4 = 18x + 6$

Since $92x + 529$ goes beyond the limit of $\mathbb{Z}_{41}$. So we need to turn it back to the limit.

$(92 - 41 * 2)x + 529 - 41 * 12 = 92x - 82x + 529 - 492 = 10x + 37\ mod\ 41$, Similarly,

$-146x - 35 = ((41 * 4) - 146)x + 41 - 35 = 18x + 6$

Step-3: X^5 mod f under $\mathbb{Z}_{41} = x * x^4$ mod $x^2 + 39x + 18$ mod 41$=(18x+6)x=18x^2+6x$

$$x^2 + 39x + 18 \Big|^{\frac{18}{18x^2+6x}}_{\frac{18x^2+702x+324}{-696x-324}} \text{ mod } 41$$

$$= \big((41 * 17) - 696\big)x + (41 * 18) - 324$$
$$= 697x - 696x + 328 - 324$$
$$= x + 4 \text{ , hence } x^5 = x + 4$$

Step-4: X^{10} mod f under $\mathbb{Z}_{41} = (x^5)^2$ mod f mod 41= $x^2 + 8x + 16$ mod $x^2 + 39x + 18$

$$x^2 + 39x + 18 \Big| \begin{array}{l} 1 \\ x^2+8x+16 \\ \underline{x^2+39x+18} \\ -31x-2 \end{array} \quad \text{mod } 41$$

$$= (41 - 31)x + 41 - 2$$
$$= 10x + 39$$
Hence $x^{10} = 10x + 39$

Step-5: X^{20} mod f under $\mathbb{Z}_{41} = (x^{10})^2$ mod f mod 41= $100x^2 + 780x + 1521$ mod f mod $\mathbb{Z}_{41}$.Since $100x^2 + 780x + 1521$ goes beyond the limit of $\mathbb{Z}_{41}$. That means I went to future, I need go back to present $(100 - 82)x^2 + (780 - 41 * 19)x + 1521 - (41*37) =$ $18x^2 + x + 4$ mod $x^2 + 39x + 18$ under $\mathbb{Z}_{41}$

$$x^2 + 39x + 18 \Big| \begin{array}{l} 18 \\ 18x^2+x+4 \\ \underline{18x^2+702x+324} \\ -701x-320 \end{array} \quad \text{mod } 41$$

$$= (738x - 701)x + 328 - 320$$
$$= 37x + 8,$$
hence $x^{20} = 37x + 8$

Step 6: X^{21} mod f under $\mathbb{Z}_{41} = x^{20}x \; mod \; f \; mod \; 41$ $(37x+8)x = 37x^2 + 8x$ mod f mod $\mathbb{Z}_{41}$,

$$x^2 + 39x + 18 \Big| \begin{array}{l} 37 \\ 37x^2+8x \\ \underline{37x^2+1443x+666} \\ -1435x-666 \end{array} \quad \text{mod } 41$$

$$= ((41 * 35) - 1435)x + 697 - 666$$
$$= 0 + 31$$

Finally x term has been vanished (surprised) leaving constant term 31. Thus $m^2 \equiv \alpha_1$ mod 41, α_p=31 and $-\alpha_p$=41-31=10(additive inverse).Let α_{p_1} =31, α_{p_2}=10. Analogously. Now, we set polynomial for $\mathbb{Z}_q$ before that we need to choose random value b (0…...q) for which we get another quadratic non residue. Previously the condition was fulfill by b=2. Now we need to choose different one rather than 2. Assuming b=4, i.e.,$(b^2 - 4a)^{\frac{q-1}{2}}$ mod 53=$(16 - 4 * 37)^{\frac{53-1}{2}}$ mod 53= (16-148)^{26} mod 53

$= ((53 * 3) - 132)^{26} = (27)^{26}$= $(27^6)^4$ 27^2 mod 53 =49*40 mod 53 = 52 that is q-1 because 53-1=52 hence choice b = 4 verifies that $\left(\frac{b^2-4a}{q}\right) = -1$ and we stick to it. So (q-1) replaced by -1. Now, we set polynomial for $\mathbb{Z}_q$.

f = x^2 – bx + α_q mod q= x^2 – 4x + 37 mod 53= x^2 + 49x + 37 mod 53. X is a variable of a polynomial and it has not particular value.

Now compute $(x)^{\frac{q+1}{2}}$ mod f=$(x)^{\frac{53+1}{2}}$ mod f that is x^{27} mod f. The binary representation of $27_{(10)} = 11011_2$. The following is an easy binary conversion technique.

Step-1: Divide 27 by 2 until the quotient 1 and ignore remainder.

Step-2: Set even number =0 and odd number =1.

Division =	1	3	6	13	27
Binary settings =	1	1	0	1	1

Now compute left to right binary exponentiation (Rules for moving from one pointer to another).

Step-1: Start from left most bit x^1 square it (x^2)

Step-2: Now move forward one bit for or a bit by bit if upcoming bit is additive identity(0), addition will be performed(x^{2+0}) means that square term unchanged else if upcoming bit is multiplicative identity(1) ,multiplication will be performed($x^2.x$)=x^3 likewise continue up to final bit.

Hence we can write 11011=x^2, x^3, x^6, x^{12}, x^{13}, x^{26} x^{27} mod f

Now compute all x^k mod f under $\mathbb{Z}_{53}$,

Step-1: X^2 mod f under $\mathbb{Z}_{53}$,

$$x^2 + 49x + 37 \Big|^{\frac{1}{x^2}}_{\overline{-49x-37}}{}^{x^2+49x+37} \bmod 53$$

$$= (53 - 49)x + 53 - 37$$

$$= 4x + 16$$

Hence $x^2 = 4x + 16 \pmod{53}$

Since $-49x - 37$ goes beyond the limit of $\mathbb{Z}_{53}$, so we need to turn it back to the limit. Means that we are out range so we need add something to move in boundary.

Step-2: X^3 mod f under $\mathbb{Z}_{53}$=$(4x + 16)x$=$4x^2$+16x mod x^2+49x+37 mod 53

$$x^2 + 49x + 37 \Big|^{\frac{4}{4x^2+16x}}_{\overline{-180x-148}}{}^{4x^2+196x+148} \bmod 53$$

$$= (212 - 180)x + 159 - 148$$

$$\therefore\ x^3 = 32x + 11 \pmod{53}$$

Step-3: X^6 mod f under $\mathbb{Z}_{53}=(32x+11)^2=1024x^2+704x+121 \bmod x^2+49x+37 \bmod 53 = 17x^2+15x+15 \bmod f \bmod 53$

$$x^2+49x+37 \overline{)\begin{array}{l}17 \\ 17x^2+15x+15 \\ \hline 17x^2+833x+629 \\ \hline -818x-614\end{array}} \bmod 53$$

$$\therefore x^6 = 30x+22 \pmod{53}$$

Step-4: X^{12} mod f under $\mathbb{Z}_{53}=(30x+22)^2=900x^2+1320x+484 \bmod x^2+49x+37 \bmod 53$

$= (900-848)x^2+(1320-1272)x+484-477=52x^2+48x+7$

$$x^2+49x+37 \overline{)\begin{array}{l}52 \\ 52x^2+48x+7 \\ \hline 52x^2+2548x+1924 \\ \hline -2500x-1917\end{array}} \bmod 53$$

$$\therefore x^{12} = 44x+44 \pmod{53}$$

Step-5: X^{13} mod f under $\mathbb{Z}_{53}=(44x+44)x=44x^2+44x \bmod x^2+49x+37 \bmod 53$

$$x^2+49x+37 \overline{)\begin{array}{l}44 \\ 44x^2+44x \\ \hline 44x^2+2156x+1628 \\ \hline -2112x-1628\end{array}} \bmod 53$$

$$\therefore x^{13} = 8x+15 \pmod{53}$$

Step-6: X^{26} mod f under $\mathbb{Z}_{53}=(8x+15)^2=64x^2+240x+225 \bmod x^2+49x+37 \bmod 53$

$= (64-53)x^2+(240-212)x+225-212=11x^2+28x+13 \bmod x^2+49x+37 \bmod 53$

$$x^2+49x+37 \overline{)\begin{array}{l}11 \\ 11x^2+28x+13 \\ \hline 11x^2+539x+407 \\ \hline -511x-394\end{array}} \bmod 53$$

$$\therefore x^{26} = 19x+30 \pmod{53}$$

Step-7: X^{27} mod f under $\mathbb{Z}_{53} = (19x+30)x=19x^2+30x \bmod x^2+49x+37 \bmod 53$

$$x^2+49x+37 \overline{)\begin{array}{l}19 \\ 19x^2+30x \\ \hline 19x^2+931x+703 \\ \hline -901x-703\end{array}} \bmod 53$$

$$= ((53*17)-901)x+39 \pmod{53}$$

$$\therefore x^{27} = 0+39 \pmod{53}$$

Finally x term has been vanished (surprised) leaving constant term 39. Thus $m^2 \equiv \alpha_q \bmod 53$, $\alpha_q=39$ and $-\alpha_q=53-39=14$(additive inverse).Let $\alpha_{q_1}=39$, $\alpha_{q_2}=14$. Now we have to calculate Bezouts coefficient for q=53 and p=41 by using Extended Euclidean algorithm. Hence, x=-17, y=22. Means that -17 is inverse of y(41-17)=24 and 22 is inverse of x. hence, u=24, v=22. Now using Chinese remainder theorem we have to calculate four conjugative roots

(R). Achieving coefficients is Bezout coefficients come from inversion technique (recursively) that is why quadratic residue modulo p and modulo q are used recursively in Chinese remainder theorem. $\text{CRT} = (\text{Bezouts coefficient}_1 * \text{private key}_1 * \text{square root}_2 + \text{Bezouts coefficient}_2 * \text{private key}_2 * \text{square root}_1) \bmod N$. as we know square root $=\pm\sqrt{}$ means that formula must be used twice one for positive root and one for negative root and therefore the CRT is as follows.

$$R_1 = \{(y * p * \alpha_{q1}) + (x * q * \alpha_{p1})\} mod\ 2173$$
$$= 22 * 41 * 39 - 17 * 53 * 31 = 35178 - 27931 = 7247\ mod\ 2173 = 728$$
$$R_2 = -R_1\ mod\ 2173 = 2173 - 728 = 1445$$
$$R_3 = \{(y * p * \alpha_{q2}) - (x * q * \alpha_{p2})\} mod\ 2173$$
$$= 22 * 41 * 14 + 17 * 53 * 10 = 12628 - 9010 = 31638\ mod\ 2173 = 2081$$
$$R_4 = -R_3\ mod\ 2173 = 2173 - 2081 = 92$$

Therefore intended message is one of the four roots (728, 1445, 2081, 92). To identify right one from four root is quit but tricky. However, it could be solution of parity bit selection or replicating biting technique. The message can be identified among four roots by choosing such roots which satisfies any one of them R_1 or R_2 or R_3 or $R_4 \equiv \pm 1 \bmod 53$ and $\equiv \pm 2 \bmod 41$.

2.2.3 Existing Research on Rabin Cipher

There are many surveys have been dedicated over Rabin's cryptosystem. Recently various modifications of Rabin's cryptosystem have been published in different scientific journals (Hardy, et.al., 1971), Identification Scheme using biquadratic residuosity. A Rabin scheme working with primes p=7 and q=11 congruent 3 modulo 4 can be defined considering the decomposition $N = v\bar{v}\ with\ v = \pi_1\pi_2$ being the product of two primary factors of p and q respectively.

`A worked out example`: the public key V, message (m) =13,
Encrypted message {C, b_0, b_1} where $C=m^2 \bmod N=15$, $b_0=m \bmod 2 =1$,

$$b_1 = \begin{cases} 1 & if \quad \left[\frac{m}{v}\right]_4 \in \{1,\ i\} \\ 0 & if \quad \left[\frac{m}{v}\right]_4 \in \{-1, -i\} \end{cases} \ldots\ldots\ldots\ldots\ldots Equ.(17)$$

$b_1=\left[\frac{13}{77}\right]_4=\left[\frac{13}{7}\right]_4\left[\frac{13}{11}\right]_4=\left[\frac{2}{7}\right]_4\left[\frac{3}{7}\right]_4\left[\frac{2}{11}\right]_4 = 1\times -1\times -1 = 1$

`Decryption Stage:` According to Congruence law, step (1, 2) is computed.

Step-1: $\frac{77}{7}$ $V_1 \equiv 1 \bmod 7 \rightarrow 11\ V_1 \equiv 1 \bmod 7 \rightarrow 2\ V_1 \equiv 1 \bmod 7 \rightarrow V_1 = 2$

Step-2: $\frac{77}{11}$ $V_2 \equiv 1 \bmod 11 \rightarrow 7\ V_2 \equiv 1 \bmod 11 \rightarrow (-3)\ V_2 \equiv 1 \bmod 11 \rightarrow V_1 = 8$

The following root computation process for deterministic polynomial time because of Blum prime formation is considered in this example.

$a_1 = C^{((p+1)/4)} \bmod p = 15^2 \bmod 7 = 1$	$a_3 = p - a_1 = 7 - 1 = 6$ inverse of a_1
$a_2 = C^{((q+1)/4)} \bmod q = 15^3 \bmod 11 = 9$	$a_4 = q - a_2 = 11 - 9 = 2$ inverse of a_2
[+ +]	[- -]

Now according to CRT, Four roots of unity is computed bellow.

Step-1: $[++]\ x \equiv 1\ mod\ 7\ and\ x \equiv 9\ mod\ 11$

$$x_1 = \left\{a_1 * V_1 * \frac{N}{p} + a_2 * V_2 * \frac{N}{q}\right\} mod\ N$$

$$= \left\{1 * 2 * \frac{77}{7} + 9 * 8 * \frac{77}{11}\right\} mod\ 77 = 527\ (77) = 64$$

Step-2: $[-+]\ x \equiv 6\ mod\ 7\ and\ x \equiv 9\ mod\ 11$

$$x_2 = \left\{a_2 * V_1 * \frac{N}{p} + a_3 * V_2 * \frac{N}{q}\right\} mod\ N$$

$$= \left\{6 * 2 * \frac{77}{7} + 9 * 8 * \frac{77}{11}\right\} mod\ 77 = 636\ (77) = 20$$

Step-3: $[+-]\ x \equiv 1\ mod\ 7\ and\ x \equiv 2\ mod\ 11$

$$x_3 = \left\{a_1 * V_1 * \frac{N}{p} + a_4 * V_2 * \frac{N}{q}\right\} mod\ N$$

$$= \left\{1 * 2 * \frac{77}{7} + 2 * 8 * \frac{77}{11}\right\} mod\ 77 = 134\ (77) = 57$$

Step-4: $[--]\ x \equiv 6\ mod\ 7\ and\ x \equiv 2\ mod\ 11$

$$x_4 = \left\{a_3 * V_1 * \frac{N}{p} + a_4 * V_2 * \frac{N}{q}\right\} mod\ N$$

$$= \left\{6 * 2 * \frac{77}{7} + 2 * 8 * \frac{77}{11}\right\} mod\ 77 = 244\ (77) = 13$$

Choose two roots specified by b_0 those are (x_3, x_4). Now compute quartic residues as follows

$$D_1 = \left[\frac{X_3}{V}\right]_4 = \left[\frac{57}{77}\right]_4 = \left[\frac{57}{7}\right]_4 \left[\frac{57}{11}\right]_4 = \left[\frac{1}{7}\right]_4 \left[\frac{2}{11}\right]_4 = 1 \times -1 = -1 = 0$$

$$D_2 = \left[\frac{X_4}{V}\right]_4 = \left[\frac{13}{77}\right]_4 = \left[\frac{13}{7}\right]_4 \left[\frac{13}{11}\right]_4 = \left[\frac{2}{7}\right]_4 \left[\frac{3}{7}\right]_4 \left[\frac{2}{11}\right]_4 = 1 \times -1 \times -1 = 1$$

https://doi.org/10.29322/ijsrp.29.12.2019

Now D_2 is equivalent to b_1. So root x_4=13 is originally decrypted message.

(Williams, 1998) proposed an implementation of the Rabin cryptosystem in 1980 using a parity bit and the Jacobi symbol. The decryption processes based on the observation is as follows.

D = $\frac{1}{2}(\frac{(p-1)*(q-1)}{4}+1)$, if b = a^2 mod N and $\left(\frac{\alpha}{N}\right)=1$, we have $b^D = \alpha\left(\frac{\alpha}{p}\right) = \alpha\left(\frac{\alpha}{q}\right)$, given that $\alpha(\frac{\phi(N)}{4}) = (\alpha\,\psi 1 + \alpha\,\psi_2)^{\frac{\phi(N)}{4}} = \alpha(\frac{\phi(N)}{4})\,\psi_1 + \alpha(\frac{\phi(N)}{4})\,\psi_2 = (\frac{a}{p})\,\psi_1 + (\frac{a}{q})\,\psi_2 = \left(\frac{\alpha}{p}\right) = \left(\frac{\alpha}{q}\right)$, as $\left(\frac{\alpha}{p}\right) = \alpha^{\frac{p-1}{2}} \bmod p$, $\left(\frac{\alpha}{q}\right) = \alpha^{\frac{q-1}{2}} \bmod q$

Public key: N, S, where S is an integer such that Jacobi $symbol\ (\frac{S}{N}) = -1$

Encrypted message: C, c_1, c_2, where $c_1 = \frac{1}{2}\left\{1 - \left(\frac{m}{N}\right)\right\}$, $m_1 = m * S^{c_1} \bmod N$,

$c_2 = m_1\ mod\ 2$, and $C = {m_1}^2\ mod\ N$.

A workout example:

Decryption stage: Receiver computes $m' = C^D \bmod N$ and $m'' = N - m'$, and choose the two roots number among four with the parity specified by c_2. The original message is recovered as opposite of $m = S^{-c_1}m''$.

Step 1: Suppose Alice and Bob are communicating each other by exchanging message. First Alice choses two random prime number p=7 and q=11 according to p≡q≡3 mod 4 privately and calculate public key N=7.11 = 77, secret key D = $\frac{1}{2}(\frac{(7-1)(11-1)}{4}+1)$ = 8. After that she will choose S such that $\left(\frac{S}{N}\right) \equiv -1$, Let S = 2 and $(\frac{2}{77}) = (\frac{2}{7})(\frac{2}{11})$ = -1. Now Alice publicizes two public keys {77, 2} and keeping D as a private key in her pocket.

Step 2: Now Bob wants to send message $(m) = 54$ to Alice. First, he will compute

$$c_1 = \frac{1}{2}\left\{1 - \left(\frac{54}{77}\right)\right\} = \frac{1}{2}\left\{1 - \left(\frac{54}{7}\right)\left(\frac{54}{11}\right)\right\} = \frac{1}{2}\left\{1-\left(\frac{6}{7}\right)\left(\frac{3^2}{7}\right)\left(\frac{6}{11}\right)\left(\frac{3^2}{11}\right)\right\}$$
$$= \frac{1}{2}\left\{1-\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)\right\} = \frac{1}{2}\left\{1-\left(\frac{3}{11}\right)\right\}, 3 \equiv 3\ mod\ 4, 11 \equiv 3\ mod\ 4$$
$$= \frac{1}{2}\left[1-\left\{-\left(\frac{11}{3}\right)\right\}\right] = 0,$$

$m_1 = 2^0 * 54\ mod\ 77 = 54,\ c_2 = 54\ mod\ 2 = 0, and$

$C = 54^2\ mod\ 77 = 67$ and then he will send tuple $(0, 0, 67)$ as a cypher text to Alice.

Step 3: $m' = C^D\ mod\ N = ((67)^4)^2\ mod\ 77 = 23, m'' = N - m' = 77 - 23 = 54$

the original message is 54 because sending parity bit of Bob is even that is why message must be even. William's Scheme work if and only if $\left(\frac{m}{N}\right) = 1\ and\ \left(\frac{S}{N}\right) = -1$. This scheme does not have solution of same quadratic residue too. Another simple variant is as follows.

`Encryption Message:` $\{C, b_0, b_1\}$, where Let the private keys are: $p = 19$ and $q = 31$,
Message (M) $= 65 =$ A (ASCII). Public key N $= 589$
$C = 65^2\ mod\ 589 = 102\ ,\ b_0 = M\ mod\ 2 = 1$, $b_1 = \frac{1}{2}\left\{1 + \frac{65}{589}\right\} = 0.5552$
A sends the triplet $(102, 1, 0.5552)$ to B.

`Decryption:` B's private keys $p = 19$ and $q = 31$ are predefined.

B computes after getting response from an entity A is as follows.

$M_p = C^{\frac{p+1}{4}}\ mod\ p = 102^5 \bmod 19 = 102^2 * 102^3 \bmod 19 = 11$

$M_q = C^{\frac{q+1}{4}}\ mod\ q = 102^8 \bmod 31 = 28$

$\lambda_1 * 19 + \lambda_2 * 31 = 1\ and\ GCD\ (31, 19) = 1$. Applying Extended Euclidean algorithm, find out $\lambda_1 = -13$, λ_2=8 and then applying Chinese remainder theorem four roots can be calculated by following ways.

$X_1 = (-13 * 19 * 28 + 8 * 31 * 11)\ mod\ 589$
$= (-6916 + 2728)\ mod\ 589 = 4712 - 4188 = 524$
$X_2 = N - X_1 = 589 - 524 = 65$
$X_3 = (-13 * 19 * 28 - 8 * 31 * 11)\ mod\ 589$
$= (-6916 - 2728)\ mod\ 589$
$= 10013 - 9644 = 369$
$X_4 = N - X_3 = 589 - 369 = 220$

Now two roots(x_2, x_3) will be selected specified by b_0 and calculate two equation

$$R_1 = \frac{1}{2}\left\{1 + \frac{x_2}{N}\right\} = \frac{1}{2}\left\{1 + \frac{65}{589}\right\} = 0.5552$$

$$R_2 = \frac{1}{2}\left\{1 + \frac{x_3}{N}\right\} = \frac{1}{2}\left\{1 + \frac{369}{589}\right\} = 0.8132$$

Now bob will match $R_1$and R_2 with b_1. Since b_1=$R_{1,}$ So original message x_2=65.

Alternatively the following approach can be applied.

$M_p = C^{\frac{(p+1)}{4}}\ mod\ p = 102^5\ mod\ 19 = 102^2 * 102^3\ mod\ 19 = 11$ $M_q = C^{\frac{(q+1)}{4}}\ mod\ q = 102^8\ mod\ 31 = 28$	U_p, U_q
$-M_p\ mod\ p = 19 - 11 = 8\ mod\ 19 = 8,$	U_{p-}, U_{q-}

$-M_q \, mod \, q \; = \; 31 \; - \; 28 \; = \; 3 \, mod \, 31 \; = \; 3$	
$n/p \; * \; v_1 \; \equiv \;\; 1 \, mod \, p \; \rightarrow \; 31 \; * \; v_1 \; \equiv \; 1 \, mod \, 19 \; \rightarrow \; v_1 \; = \; 8$	V_1
$n/q \; * \; v_2 \; \equiv \;\; 1 \, mod \, q \; \rightarrow \; 19 \; * \; v_2 \; \equiv \;\; 1 \, mod \, 31 \; \rightarrow \; v_2 \; = \; 18$	V_2

Finally, by applying the Chinese remainder theorem, four square roots has to be computed and the system of congruence $x \; \equiv \; u_{\mathrm{i}} \; * v_{\mathrm{i}} \; \frac{n}{n_i}$ is as follows:

Step-1: $x \; \equiv \;\; 11 \, mod \, 19 \; and \; x \; \equiv \;\; 28 \, mod \, 31$:

$$x \; = \; (u_p \; * \; v_1 \; * \; \frac{N}{p} \; + \; u_q \; * \; v_2 \; * \; \frac{N}{q}) \; mod \; N$$

$$= \; (11 * 8 * 31 \; + \; 28 * 18 * 19) \; mod \; 589$$

$$= 12304 \; mod \; 589$$

$$= 524$$

Step-2: $x \; \equiv \;\; 8 \, mod \, 19 \; and \; x \; \equiv \;\; 28 \, mod \, 31$:

$$x \; = \; (u_p \; * \; v_1 \; * \; \frac{N}{p} \; + \; u_q \; * \; v_2 \; * \; \frac{N}{q}) \; mod \; N$$

$$= \; (8 * 8 * 31 \; + \; 28 * 18 * 19) \; mod \; 589$$

$$= \; 11560 \; mod \; 589$$

$$= 369$$

Step-3: $x \; \equiv \;\; 11 \, mod \, 19 \; and \; x \; \equiv \;\; 3 \, mod \, 31$:

$$x \; = \; (u_p \; * \; v_1 \; * \; \frac{N}{p} \; + \; u_q \; * \; v_2 \; * \; \frac{N}{q}) \; mod \; N$$

$$= \; (11 * 8 * 31 \; + \; 3 * 18 * 31) \; mod \; 589$$

$$= \; 4402 \; mod \; 589$$

$$= \; 279$$

Step-4: $x \; \equiv \;\; 8 \, mod \, 19 \; and \; x \; \equiv \;\; 3 \, mod \, 31$:

$$x \; = \; (u_p \; * \; v_1 \; * \; \frac{N}{p} \; + \; u_q \; * \; v_2 \; * \; \frac{N}{q}) \; mod \; N$$

$$= \; (8 * 8 * 31 \; + \; 3 * 18 * 19) \; mod \; 589 = \; 3010 \; mod \; 589 \; = \; 65$$

Finally, the original message must be among the 524, 369, 279 *and* 65, *As* $b_0 = 1$,

we take the 2 roots specified by b_0, as $\mathrm{x} \; = \; 67, \mathrm{y} \; = \; 181$.

Now $\mathrm{r} \; = \; \frac{1}{2}\left\{1 + \frac{x}{n}\right\} = \frac{1}{2}\left\{1 + \frac{67}{589}\right\} = \; 0.556876$

And $\mathrm{s} \; = \; \frac{1}{2}\left\{1 + \frac{y}{n}\right\} = \frac{1}{2}\left\{1 + \frac{181}{589}\right\} = \; 0.653650$

Now $\mathrm{b} = 0.556876, \mathrm{r} \; = \; \mathrm{b}$, the message $\mathrm{M} \; = \; \mathrm{x} \; = \; 67$,

So the Plaintext $\mathrm{P} \; = \; (\mathrm{M} - \mathrm{K_s}) \; = \; (67 - 24) \; = \; 43$

(Elia, M. et al., 2013) implemented a solution of Rabin's Cryptosystem using Dedekind Sum. The implemented techniques are described as follows.

Encrypted message:

{C, b_0, b_1}, where $C = m^2 \, mod \, N \; = \; 13^2 \, mod \, 77 \; = \; 15. N = p * q = 7 * 11 = 77$

$b_0 = \; m \, mod \, 2 = 13 \, mod \, 2 \; = \; 1, b_1 = \; S \, (13, 77) \, mod \, 8.$

$b_1 = \; 77 + 1 - 2 \left(\frac{13}{77}\right) \bmod 8 \; = \; 78 - 2 \left(\frac{13}{7}\right)\left(\frac{13}{11}\right) \bmod 8 \; = 78 - 2 \left(\frac{6}{7}\right)\left(\frac{2}{11}\right) mod \, 8$

$= 78 - 2 \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)(-1) \bmod 8 = 78 - 2 \, (1)(1) \bmod 8 = (78 - 2) \bmod 8 = \; 4$

Decryption stage:

Receiver computes $\lambda_1 \; = \; -3 \; and \; \lambda_2 \; = \; 2$ by extended Euclidean algorithm and Roots are as follows.

$$u_1 = \; C^{\frac{(p+1)}{4}} \; mod \, p \; = \; 15^{\frac{(7+1)}{4}} \, mod \, 7 \; = 1$$

$$u_2 = \; C^{\frac{(q+1)}{4}} \; mod \, q \; = 15^{\frac{(11+1)}{4}} \, mod \, 11 \; = \; 9$$

Now calculate four roots using Chinese Remainder theorem

$X_1 = (p * \lambda_1 * u_2 + q * \lambda_2 * u_1) \, mod \, N = (7 * -3 * 9 + \; 11 * 2 * 1) \, mod \, 77 \; = \; 64$

$X_2 \; = \; N \; - \; X_1 \; = \; 77 \; - \; 64 \; = \; 13$

$X_3 = (p * \lambda_1 * u_2 - q * \lambda_2 * u_1) \, mod \, N = (7 * -3 * 9 - 11 * 2 * 1) \, mod \, 77 \; = \; 20$

$X_4 \; = \; N \; - \; X_3 \; = \; 77 \; - \; 20 \; = \; 57$

Choose two roots specified by b_0 that's are (X_2, X_4) now apply Dedekind sum on $X_2 = D_2 \; = \; S(13,77) and$

$X_4 \; = \; D_4 \; = \; S(57,77)$

Computation:

$$X_2 = D_2 = \; S \, (13, 77)$$
$$= \; 77 + 1 - 2 \left(\frac{13}{77}\right) \, mod \, 8$$
$$= \; 78 - 2 \left(\frac{13}{7}\right)\left(\frac{13}{11}\right) mod \, 8$$
$$= \; 78 - 2 \left(\frac{6}{7}\right)\left(\frac{2}{11}\right) \, mod \, 8$$
$$= \; 78 - 2 \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) \; (-1) \, mod \, 8$$
$$= \; 78 - 2 \, (1) \, (-1) \, (-1) \, mod \, 8$$
$$= \; (78 \; - 2) \, mod \, 8 \; = 4$$

$$X_4 = D_4 = S \, (57, 77)$$
$$= \; 77 + 1 - 2 \left(\frac{57}{77}\right) \, mod \, 8$$
$$= \; 78 - 2 \left(\frac{57}{7}\right)\left(\frac{57}{11}\right) \, mod \, 8$$
$$= \; 78 - 2 \left(\frac{1}{7}\right)\left(\frac{2}{11}\right) \, mod \, 8$$
$$= \; 78 \; - 2 \, (1) \, (-1) \, mod \, 8$$
$$= \; 80 \; mod \, 8 = 0$$

Receiver accept the original message by comparing tow Dedekind sum D_2 and D_4 with b1. It can be seen that $b_1 = D_2 = X_2$ means that 13 is the right plaintext. This can be expressed using congruence law is as follows.

Step-1: $\frac{77}{7}V_1 \equiv 1 \bmod 7 \rightarrow 11\,V_1 \equiv 1 \bmod 7 \rightarrow 2\,V_1 \equiv 1 \bmod 7 \rightarrow V_1 = 2$

Step-2: $\frac{77}{11}V_2 \equiv 1 \bmod 11 \rightarrow 7\,V_2 \equiv 1 \bmod 11 \rightarrow (-3)V_2 \equiv 1 \bmod 11 \rightarrow V_2 = 8$

The following root computation process for deterministic polynomial time because of Blum prime formation is considered in this example.

$a_1 = C^{\frac{(p+1)}{4}} \bmod p = 15^2 \bmod 7 = 1$	$a_3 = p - a_1 = 7 - 1 = 6$ inverse of a_1.
$a_2 = C^{\frac{(q+1)}{4}} \bmod q = 15^2 \bmod 11 = 9$	$a_4 = q - a_2 = 11 - 9 = 2$ inverse of a_2
$[++]$	$[--]$

According to CRT, four roots are calculated bellow.

Step-1: $[++]$ $x \equiv 1 mod\ 7\ and\ x \equiv 9\ mod\ 11$

$$x_1 = \left\{a_1 * V_1 * \frac{N}{p} + a_2 * V_2 * \frac{N}{q}\right\} mod\ N$$
$$= \left\{1 * 2 * \frac{77}{7} + 9 * 8 * \frac{77}{11}\right\} mod\ 77 = 527\ (77) = 64$$

Step-2: $[-+]$ $x \equiv 6\ mod 7\ and\ x \equiv 9\ mod\ 11$

$$x_2 = \left\{a_2 * V_1 * \frac{N}{p} + a_3 * V_2 * \frac{N}{q}\right\} mod\ N$$
$$= \left\{6 * 2 * \frac{77}{7} + 9 * 8 * \frac{77}{11}\right\} mod\ 77 = 636\ (77) = 20$$

Step-3: $[+-]$ $x \equiv 1 mod\ 7\ and\ x \equiv 2\ mod\ 11$

$$x_3 = \left\{a_1 * V_1 * \frac{N}{p} + a_4 * V_2 * \frac{N}{q}\right\} mod\ N$$
$$= \left\{1 * 2 * \frac{77}{7} + 2 * 8 * \frac{77}{11}\right\} mod\ 77 = 134\ (77) = 57$$

Step-4: $[--]$ $x \equiv 6 mod 7\ and\ x \equiv 2\ mod\ 11$

$$x_4 = \left\{a_3 * V_1 * \frac{N}{p} + a_4 * V_2 * \frac{N}{q}\right\} mod\ N$$
$$= \left\{6 * 2 * \frac{77}{7} + 2 * 8 * \frac{77}{11}\right\} \bmod 77 = 244\ (77) = 13$$

Choose two roots specified by b_0 that's are (X_3, X_4)now apply Dedekind sum on $D_3 = S\ (X_3, 77) and$ $D_4 = S\ (X_4, 77)$. The computation process is as follows:

$D_3 = S(57,77)$
$= 77 + 1 - 2\left(\frac{57}{77}\right) \ mod\ 8$
$= 78 - 2\left(\frac{57}{7}\right)\left(\frac{57}{11}\right) \text{mod } 8$
$= 78 - 2\left(\frac{1}{7}\right)\left(\frac{2}{11}\right) \ mod\ 8$
$= 78 - 2\,(1)\,(-1) \ mod\ 8$
$= 80 \ mod\ 8 \ = \ 0$

$D_4 = S(13,77)$
$= 77 + 1 - 2\left(\frac{13}{77}\right) \ mod\ 8$
$= 78 - 2\left(\frac{13}{7}\right)\left(\frac{13}{11}\right) \ mod\ 8$
$= 78 - 2\left(\frac{6}{7}\right)\left(\frac{2}{11}\right) \ mod\ 8$
$= 78 - 2\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)(-1) \ mod\ 8$
$= 78 - 2\,(1)\,(-1)\,(-1) \ mod\ 8$
$= (78 - 2) \ mod\ 8 \ = \ 4$

Receiver accept the original message by comparing tow Dedekind sum (D_3, D_4) with b_1. It can be seen that $b_1 = D_4 = X_4$ means that 13 is the right plaintext. Alternatively , receiver accept the original message by selecting two roots (X_3, X_4) among four specified by parity bit b_0 compute following equation to select right one

$$R_1 = \frac{1}{2}\left\{1 + \frac{X_3}{77}\right\} = \frac{1}{2}\left\{1 + \frac{57}{77}\right\} = 0.87013$$

$$R_2 = \frac{1}{2}\left\{1 + \frac{X_4}{77}\right\} = \frac{1}{2}\left\{1 + \frac{13}{77}\right\} = 0.58442$$

R_2 is equivalent to b_1, so Root $X_4 = 13$ is the right plaintext revealed. They also show another deterministic variant of Rabin cryptosystem which is as follows.

Public-key: 1st public key N, 2nd public key ξ, where $\xi = \alpha^2\,(\psi_1 - \psi_2)$ is an integer.

Encrypted message:

C For 1st round, (C_E, c_2) for 2nd round, $C = m^2 \ mod\ N$. $C_1 = \frac{1}{2}\left\{1 - \left(\frac{m}{N}\right)\right\}$,

$C_2 = m \ mod\ 2$, $C_E = C\,(-1)^{c_1}\,\xi^{c_2} \ mod\ N$

Decryption stage:

Receiver computes four square roots and chooses the two roots among four with the parity specified by C_2. After that, he neglects one which is equivalent to C_E from selected two roots and accepts remaining root as an original message.

A workout example:

Round 1st: At the initial round, Alice publicizes one public key and Bob generates an encryption key using Alice's public key and then sends it to Alice. Suppose Alice and Bob are communicating each other by exchanging message. Alice choses two random prime number p=7 and q=11 according to $p \equiv q \equiv 3 \ mod\ 4$ privately and calculate public

key $N = 7 * 11 = 77$, Alice publicizes 1st public keys 77 keeping secret key in her pocket. Then Bob generates initial encryption message $C = 13^2 \, mod \, 77 = 15$ using the public key of Alice and send it to her.

Round 2nd: In this round, Alice publicizes 2nd public key after receiving first encrypted message from Bob, on the other hand, Bob generates another encrypted message which helps Alice to identify actual message using Alice's 2nd public key and then sends it to Alice. She computes another public key using Euclidean Algorithm and Bob's encryption message 15 is as follows:

First of all the conditions $\lambda_1 * p + \lambda_2 * q = 1 \, and \, GCD\,(p, q) = 1$ must be true. These λ_1 , λ_2 are Bezout's identity. $\psi_1 = \lambda_2 * q = 22, \psi_2 = \lambda_1 * p = -21$, Let, new public key $\xi = 15^2\,(\psi_1 - \psi_2)\, mod\, N = 15^2\,(22 + 21)\, mod\, 77 = 50$ and declare 50 as a 2nd public key. The following root computation process for deterministic polynomial time because of Blum prime formation is considered in this example.

$$\alpha_1 = (C_E)^{\frac{(p+1)}{4}}\,(mod\, p) \equiv (15)^2\,(mod\, 7) \equiv 1$$

$$\alpha_2 = (C_E)^{\frac{(q+1)}{4}}\,(mod\, q) \equiv (15)^3\,(mod\, 11) \equiv 9$$

She will compute four roots using CRT.

$Y_1 = (\alpha_2\psi_1 + \alpha_1\psi_2)\, mod\, N = 9 * (-21) + 1 * 22)\, mod\, 77 = 64.$

$Y_2 = N - Y_1 = 77 - 64 = 13.$

$Y_3 = (\alpha_2\psi_1 + \alpha_1\psi_2) mod\, N = 9 * (-21) - 1 * 22)\, mod\, 77 = 20$

$Y_4 = N - Y_3 = 77 - 20 = 57$

Bob re-encrypts message using both public key of Alice as follows.

$$C_1 = \frac{1}{2}\left\{1 - \left(\frac{13}{77}\right)\right\} = \frac{1}{2}\left\{1 - \left(\frac{13}{7}\right)\left(\frac{13}{11}\right)\right\} = \frac{1}{2}\left\{1 - \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{2}{11}\right)\right\} = 0$$

$C_2 = 13\, mod\, 2 = 1, C_E = C\,(-1)^{c_1} * 50^{c_2}\, mod\, N = 15\,(-1)^0 * 50^1\, mod\, 77 = 57$

Now Bob will send 2nd encrypted message as a pair (C_E, C_2) to Alice. Finally, Alice selects two roots (13, 57) specified by parity bit C_2 among four and reject one root (57) specified C_E. So remaining 13 will be accepted as a valid message by intended receiver.

(Hasim, 2014) proposed an update methodology that used three private keys instead of two. Consequently, the eight non-deterministic plaintext generates from one cypher text. One of them is real plaintext. The advantage of this technique is to make confusing attacker while it is very annoying to receiver as extra effort is required to distinguish original plaintext out of eight text. The name of the technique initiated by author name. The description of techniques are as follows.

Encryption of H-Rabin cryptosystem:

The key-generation process of H- Rabin crypto system is as the following: Choose three large distinct primes $p, q\ and\ r$. However the scheme works with any primes, choose $p \equiv q \equiv r \equiv 3\ (mod\ 4)$ to simplify the computation of square roots modulo p, q and r. Let N the public key such that N = $(p * q * r)$ where the primes p, q and r are the private key. To encrypt a message only the public key N is needed, thus a cipher text is produced out of the original plaintext. To decrypt a cipher text the factors p, q and r of N are needed. The encryption process of H-Rabin cryptosystem is as the following:

Let $P = \{0, 1, 2 \ldots N - 1\}$ be the plaintext space (consisting of numbers)

Let $m \in P = \{0, 1, 2 \ldots N - 1\}$ be the plaintext

Let C be the cipher text that can be computed by, $C = e_k\ (m) \equiv m^2\ (mod\ N)$

Now the encoded message can be sent as C. Once the message reaches the destination, it must be decrypted.

Decryption of H-Rabin cryptosystem:

To decode the cipher text, the private keys are necessary. For that reasons, use the decryption function d_g **(c)** = $\sqrt{c}$ (mod N). Since the encryption function e_k is not an injection function, the decryption is not ambiguous. There exist eight square roots of c mod N ($c \equiv m^2\ mod\ N$), so there are eight possible messages. The decryption try to determine m such that: $C \equiv m^2\ (mod\ N)$ which is equivalent to solving the three congruence:

$$Z^2 \equiv c\ (mod\ p), \quad m_p \equiv C^{\frac{(p+1)}{4}}\ (mod\ p)$$

$$Z^2 \equiv c\ (mod\ q), \quad m_q \equiv C^{\frac{(q+1)}{4}}\ (mod\ q)$$

$$Z^2 \equiv c\ (mod\ r) \quad m_r \equiv C^{\frac{(r+1)}{4}}\ (mod\ r)$$

Finally, the eight square roots of c mod n can be computed applying the Chinese remainder theorem to the system of congruence: $+ m_p\ (mod\ p), - m_p\ \ (mod\ p), + m_q\ \ (mod\ q), - m_q\ \ (mod\ q), + m_r\ \ (mod\ r), - m_r\ \ (mod\ r)$

A workout Example:

Let $N = 1463 = p * q *. r = 7 * 11 * 19$ and m = 41. First, the message m must be encrypted using the encryption function: $C = e_k\ (m) = m^2\ (mod\ N) = 41^2\ mod\ 1463 = 218$

The encrypted message C = 218 is sent to the receiver. The receiver must decrypt the message C and has to find the eight square roots of 218 modulo 7, modulo 11 and modulo 19. The following root computation process for deterministic polynomial time because of Blum prime formation is considered in this example.

$$m_p \equiv C^{\frac{(p+1)}{4}}\ mod\ p \equiv (218)^{\frac{(7+1)}{4}}\ mod\ 7 \equiv 1$$

$$m_q \equiv C^{\frac{(q+1)}{4}}\ mod\ q \equiv (218)^{\frac{(11+1)}{4}}\ mod\ 11 \equiv 3$$

$$m_r \equiv C^{\frac{(r+1)}{4}}\ mod\ r \equiv (218)^{\frac{(19+1)}{4}}\ mod\ 19 \equiv 16$$

The system of congruence, $x = a_i b_i \frac{M}{m_i}$ is as follows

$+ m_p \ (mod\ p) \ \equiv 1 (mod\ 7)$

$- m_p \ (mod\ p) \ \equiv 6 (mod\ 7)$

$+ m_q \ (mod\ q) \ \equiv 3 (mod\ 11)$

$- m_q \ (mod\ q) \ \equiv 8 (mod\ 11)$

$+ m_r \ (mod\ r) \ \equiv 16 (mod\ 19)$

$- m_r \ (mod\ r) \ \equiv 3 (mod\ 19)$

Finally, we can apply the Chinese remainder theorem to compute the eight roots: First of all, we compute b_1, b_2 and b_3 such:

Computation: $\frac{N}{7} b_1 \equiv 1 \ (\text{mod } 7) \rightarrow 209\, b_1 \equiv 1 \ (\text{mod } 7) \rightarrow 6\, b_1 \equiv 1 (\text{mod } 7) \rightarrow b_1 = 6$

Computation: $\frac{N}{11} b_2 \equiv 1 \ (\text{mod } 11) \rightarrow 133 b_2 \equiv 1 \ (\text{mod } 11) \rightarrow 6\, b_2 \equiv 1 (\text{mod } 11) \rightarrow b_2 = 1$

Computation: $\frac{N}{19} b_3 \equiv 1 \ (\text{mod } 19) \rightarrow 77\, b_3 \equiv 1 \ (\text{mod } 19) \rightarrow 6\, b_3 \equiv 1 (\text{mod } 19) \rightarrow b_3 = 1$

Now according to CRT, four roots can be computed as follows.

Step-1: $x \equiv 1 (mod\ 7), x \equiv 3 (mod\ 11)$ *and* $x \equiv 16 (mod\ 19)$:

$$x_1 = \left\{a_1 b_1 \frac{M}{p} + a_2 b_2 \frac{M}{q} + a_3 b_3 \frac{M}{r}\right\} mod\ N$$

$$x_1 = \{(1)\ (6)\ (11 * 19) + (3)\ (1)\ (7 * 19) + (16)\ (1)\ (7 * 11)\}\ mod\ 1463$$

$$x_1 = 2885\ mod\ 1463 = 1422$$

Step-2: $x \equiv 6 (mod\ 7), x \equiv 3 (mod\ 11)$ *and* $x \equiv 16 (mod\ 19)$:

$$x_2 = \left\{a_1 b_1 \frac{M}{p} + a_2 b_2 \frac{M}{q} + a_3 b_3 \frac{M}{r}\right\} mod\ N$$

$$x_2 = \{(6)\ (6)\ (11 * 19) + (3)\ (1)\ (7 * 19) + (16)\ (1)\ (7 * 11)\}\ mod\ 1463$$

$$x_2 = 9155\ mod\ 1463 = 377$$

Step-3: $x \equiv 1 (mod\ 7), x \equiv 8 (mod\ 11)$ *and* $x \equiv 16 (mod\ 19)$:

$$x_3 = \left\{a_1 b_1 \frac{M}{p} + a_2 b_2 \frac{M}{q} + a_3 b_3 \frac{M}{r}\right\} mod\ N$$

$$x_3 = \{(1)\ (6)\ (11 * 19) + (8)\ (1)\ (7 * 19) + (16)\ (1)\ (7 * 11)\}\ mod\ 1463$$

$$x_3 = 3550\ mod\ 1463 = 624$$

Step-4: $x \equiv 1(mod\ 7), x \equiv 3(mod\ 11)\ and\ x \equiv 3(mod\ 19)$:

$$x_4 = \left\{ a_1 b_1 \frac{M}{p} + a_2 b_2 \frac{M}{q} + a_3 b_3 \frac{M}{r} \right\} mod\ N$$

$$x_4 = \{(1)\ (6)\ (11 * 19) + (3)\ (1)\ (7 * 19) + (3)\ (1)\ (7 * 11)\}\ mod\ 1463$$

$$x_4 = 1884\ mod\ 1463 = 421$$

Now, we can take the advantage of symmetry to get the other results:

Step-5: $x_5 = 1463 - 1422 = 41.$

Step-6: $x_6 = 1463 - 377 = 1086.$

Step-7: $x_7 = 1463 - 624 = 839.$

Step-8: $x_8 = 463 - 421 = 1042.$

Finally, the original message must be in following sequence. $1422, 377, 624, 421, 41, 1086, 839\ and\ 1042$. The drawback of Deterministic Rabin Cryptosystem is that, it is applicable for an odd length message. In case of even length message, it can't justify the original plaintext as replicated bit or repeated pattern cannot be noticed in any of four options.

(Chakraborty, et.al., 2014) designed a hybrid Rabin Cryptosystem adding message authentication logic from Needham–Schroeder protocol (*Roger,et.al.,1978,* Waite, et.al., 1987). Hybrid Rabin Cryptosystem designed using a combination of Symmetric and asymmetric key that was why it was called hybrid. The technique can be described as follows.

`Round 1:` The sender A uses the receiver B's public key to encrypt a message to the receiver containing to the receiver containing an identifier of A (ID_A) and a nonce N_1 which is used to identify this transaction uniquely. B sends a message to A encrypted with PU_A and A's nonce as well as a new nonce N_2 generated by B. A returns N_2 Using B's public key. A selects secret key K_s and sends $M = E(PUb, E(PRa, Ks))$ to B. B computes $D(PUa, D(PRb, M))$ to recover the secret key.

`Round 2:` The N is the public key which is the multiplication of p and q where p and q are both private keys and both p and q are congruent to 3 mod 4. A prepares the message M by adding his shared secret key with the plaintext and then applying the encryption function $C = M^2\ mod\ N$. A further calculates 2 more values $a\ and\ b$ such that $a = M\ mod\ 2\ and\ b = \frac{1}{2}(1 + \frac{M}{N})$. for decryption B has to use the Chinese Remainder Theorem to get the four square roots. At first B has to calculate $M_p\ and\ M_q$ such that $M_p = C^{\frac{(p+1)}{4}} \text{mod p}$ and $M_q = C^{\frac{(q+1)}{4}} \text{mod q}$. Then B has to compute $+M_p\ mod\ p, -M_p\ mod\ p, +M_q\ mod\ q\ and\ -M_q\ mod\ q$. These are the 4 square roots. Then take the two roots having the same parity specified by a, say x and y. Compute the numbers $\frac{1}{2}\left(1 + \frac{x}{n}\right)\ and \frac{1}{2}\left(1 + \frac{y}{n}\right)$. Then take the root corresponding to the number equal to the value of b. Thus the message M is retrieved. Now B has to subtract the shared secret key from M to retrieve the plaintext.

A workout Example: The Modified Rabin Cryptosystem Sharing the Secret key is as follows. Let the $ID\ of\ A = 1001\ and\ the\ ID\ of\ B = 1002$. A sends ID and nonce $N_1 = 311$ encrypted with the public key of $B, i.e.E\ (PU_B(1001||311))\ to\ B$. B sends nonce

$N_1\ and\ N_2 = 653$ Encrypted with the public key of $A, i.e.E\ (PU_A\ (311||653))$ to A. A sends the nonce N_2 encrypted with the public key of $B\ i.e.E\ (PU_B, 653)\ to\ B$. A then encrypts the secret key K_S to be shared with his own private key and then again encrypt it with the public key of B and sends $X = E\ (PU_B, E\ (PR_A, K_S))\ to\ B$. B computes $D(PU_A,\ D(PR_B,\ X))$ to recover the secret key.

Encryption:

Let A wants to send the plaintext $P_t = 43$ and the secret key $K_s = 24$

Then the message $M = (P_t + K_s) = (43 + 24) = 67$.

Let the public key $n = 589$

Then the cipher text $C = E\ (67, 589) = 67^2 \bmod 589 = 366$.

$a = M \bmod 2 = 67 \bmod 2 = 1,\ b = \frac{1}{2}\left\{1 + \frac{M}{N}\right\} = \frac{1}{2}\left\{1 + \frac{67}{589}\right\} = 0.556876$

A sends the triple $(366, 1, 0.556876)$ to B

Decryption:

Let the private keys are: $p = 19\ and\ q = 31\ Public\ key\ N = 589$. The following root computation process for deterministic polynomial time because of Blum prime formation is considered in this example. B's computation process is as follows.

$M_p = C^{\frac{(p+1)}{4}} \bmod p = 3665 \bmod 19 = 9$ $M_q = C^{\frac{(q+1)}{4}}) \bmod q = 3668 \bmod 31 = 5$	U_1
$-M_p\ mod\ p = 19 - 9 = 10\ mod\ 19 = 10$ $-M_q\ mod\ q = 31 - 5 = 26\ mod\ 31 = 26$	U_2
$n/p * v_1 \equiv 1 \bmod p \rightarrow 31 * v_1 \equiv 1 \bmod 19 \rightarrow v_1 = 8$	V_1
$n/q * v_2 \equiv 1 \bmod q \rightarrow 19 * v_2 \equiv 1 \bmod 31 \rightarrow v_2 = 18$	V_2

Finally, by applying the Chinese remainder theorem to compute the four square roots and the system of congruence $x \equiv u_i * v_i * \frac{n}{n_i}$ is as follows:

Step-1: $x \equiv 9\ mod\ 19\ and\ x \equiv 5\ mod\ 31$:

$$x_1 = \left\{u_1 * v_1 * \frac{N}{P} + u_2 * v_2 * \frac{N}{q}\right\} mod\ N$$
$$= \{9 * 8 * 31 + 5 * 18 * 19\}\ mod\ 589$$
$$= 3942\ mod\ 589$$
$$= 408$$

Step-2: $x \equiv 10\ mod\ 19\ and\ x \equiv\ 5\ mod\ 31$:

$$x_2 = \left\{ u_1 * v_1 * \frac{N}{P} + u_2 * v_2 * \frac{N}{q} \right\} mod\ N$$
$$= \{10 * 8 * 31 + 5 * 18 * 19\}\ mod\ 589$$
$$= 4190\ mod\ 589$$
$$= 67$$

Step-3: $x \equiv 9\ mod\ 19\ and\ x \equiv 26\ mod\ 31$:

$$x_3 = \left\{ u_1 * v_1 * \frac{N}{P} + u_2 * v_2 * \frac{N}{q} \right\} mod\ N$$
$$= \{9 * 8 * 31 + 26 * 18 * 31\}\ mod\ 589$$
$$= 11124\ mod\ 589$$
$$= 522$$

Step-4: $x \equiv 10\ mod\ 19\ and\ x \equiv 26\ mod\ 31$:

$$x_4 = \left\{ u_1 * v_1 * \frac{N}{P} + u_2 * v_2 * \frac{N}{q} \right\} mod\ N$$
$$= \{10 * 8 * 31 + 26 * 18 * 19\}\ mod\ 589$$
$$= 11372\ mod\ 589$$
$$= 181$$

Finally, the original message must be among the 408, 67, 522 or 181. As a = 1, we take the 2 roots specified by a which are x = 67, y = 181, Now r $= \frac{1}{2}\left\{1 + \frac{x}{n}\right\} = \frac{1}{2}\left\{1 + \frac{67}{589}\right\} =$ 0.556876 and s $= \frac{1}{2}\left\{1 + \frac{y}{n}\right\} = \frac{1}{2}\left\{1 + \frac{181}{589}\right\} =$ 0.653650. Now b = 0.556876 as r = b, message M = x = 67, so the Plaintext P= $(M - K_s) = (67 - 24) = 43$. (Sattar, et.al, 2015) showed an extended application of Michael O. Rabin Cryptosystem in the field of cryptography to steganography. In Michael O. Rabin cryptosystem produce four decryption results among one of them is correct and other three are pseudo results. In the steganography application, a benefit of the illusions messages generated from Rabin's cryptosystem were taken by authors. Although, in cryptographic application, those three false results are considered as a weakness point of Rabin Cryptosystem owing to size problems. The authors in this articles turned Rabin Cryptosystem's disadvantage to advantage in steganography which will be used not only constructing hiding map but also authenticated mechanisms which guide the hiding process. The authors of this article converted secret message into ASCII value and used it in Rabin encryption algorithm which gives the system encrypted message that will represent the input to the decryption algorithm. The procedure produce four message. One of them is secret message and the rest are illusion messages with a different length that constructs the map is as below:

`The pseudo code for determining Map`

$i = 0$, $While\ (m_i <> c)\ do$, $Hiding\ map = m_i$, End. Preparation of color cover image for hiding c is shown as follows.

`Hiding Algorithm:`

Input: Cipher message (Text)

Cover Image (Image)

Map (binary format)

Output: $Stego - object$

https://doi.org/10.29322/ijsrp.29.12.2019

The Entire process follow some important steps.

- Read secret message
- Convert secret to binary format.
- Read Cover color image and get three bands (Red, Green, Blue).
- Convert all band of RGB to binary format.
- Get based on Map (Output of decryption)
- For each byte band do the following steps.
- Prepare a Target address through the following equation.
    - $Target\ Address\ (T) = (1 * K_1 + 2 * K_2 + 4 * K_3)\ mod\ 3$
    - Replacing the target address bit with the secret bit message.
- Go to step 6 until hide all the secret.
- At the end gather all the bands to form $stegoobject$.

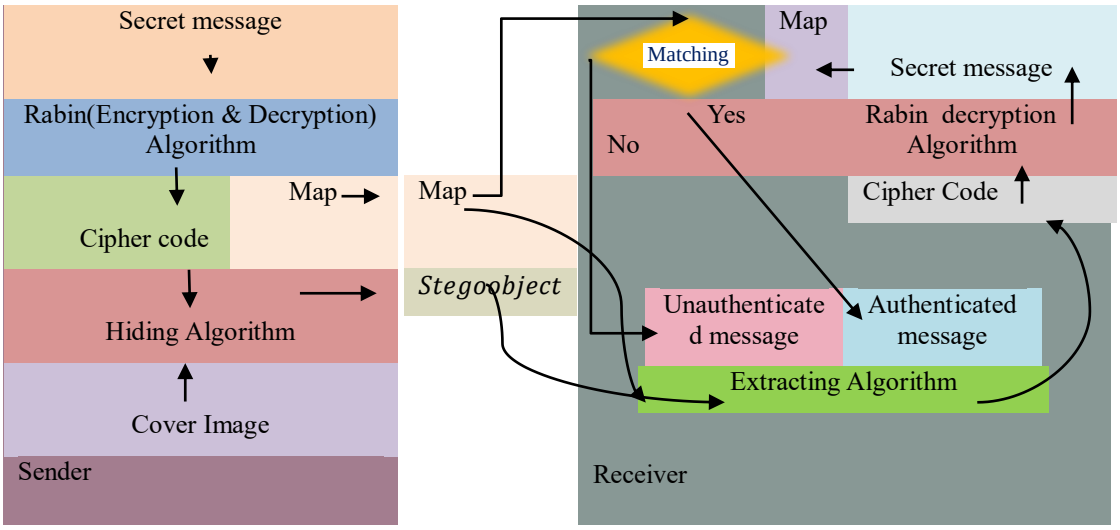


Figure 2.4: The block diagram of the $stegoobject$

It show a good result for guiding hiding mechanism and authentication mechanism. Both of the map and stegoobject will transmit through channel from sender to receiver which has shown in figure 8. When the receiver get both of them will start extract ciphertext and decrypt to get four message $\{m_1, m_2, m_3, m_4\}$ here one of them is a secret message and rest are for constructing a map that will work as a guide for hiding mechanism and this can easy to filter because of having map available. If the extracted map matched the received one that is authenticated otherwise it rejects and this is easy to filter because of having map available.

(Kaminaga, et.al. 2016) discussed a fault attack technique on modular exponentiation of Rabin's encryption where a complicated situation arose in case of message reconstruction when message and the public key were not relatively prime. They also provided a rigorous algorithm to handle message reconstruction. They provided a fundamental idea about two attacks on crashing modulus on modular squaring for Rabin Cryptosystem. The attack are performed attacker when public key moves from nonvolatile memory to register byte by byte. Their assumption attacker can inject one byte fault into this moving process. Their simulation result shows that only 14.4% success rate in Transient attack and 54% success rate for injection attack for small prime which is actually negligible because real life prime number so big. Their attack models are as follows.

Transient fault attack:

Let $Z\{a,b\}$ be a set of integers in the interval $\{a,b\}$. Assuming that the attacker can inject a transient fault that public key N modifies by byte, that is, the injected fault affects only one byte of the public key by modifying it randomly as follows: $N\hat{} = N \oplus \epsilon\, where \oplus$ is bitwise exclusive OR and $\epsilon = R_i * 2^{8i}, R_i \in Z\{1, 2^8 - 1\}\, for\ i \neq 0$ which is required to preserve the parity of $N\hat{}$. Suppose the attacker knows the position i, but the correct value of the faulty public key N$\hat{}$ is unknown by the attacker. The attacker must factor $255 (= 28 - 1)\ candidates\ of\ N\hat{}$. Attack also works for a fault that affects several bytes of N. However, the attacker's task grows in proportion to the number of candidates N$\hat{}$ of perturbed N. This is a natural assumption for both WIPR and RAMON. In the WIPR case, the attack target is the time at which i-th byte $N[i]\ of\ N$ moves from non-volatile memory to the register for multiplication before multiplying r and N.

Instruction skipping attack:

The second fault model is based on the instruction skip technique. Instruction skip is equivalent to replacing an instruction with a no operation in assembly language. Instruction skip does not affect the registers, internal memory, and calculation process. It is possible to reconstruct an entire secret exponent with 63(=26-1). Implementation with the 26-ary method using instruction skipping technique in pre-computation phase. Their attack target is a conditional branch operation for moving the last byte of N at the counter $i = 127.$ if the conditional branch operation is skipped, the attacker obtains the faulted public key $\hat{}$ N as follows:

$$N\hat{} = \sum_{i=0}^{126} N[i]2^{8i} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Equ(18)$$

Where each $N[i] \in Z\,(0{,}255)$. Clearly, N$\hat{}$ is one byte shorter than the original N, and preserves its parity. In this case, N$\hat{}$ is uniquely determine. Therefore, from the computational point of view, attack for this case is easier than the attack for the 'crash a byte of N' case. The notion of first attack model were actually derived from (Berzati, et.al., 2008, Berzati,et.al., 2009).

(Chandrakar, et.al. 2017) developed a secure two factor remote authentication scheme using the Rabin Cryptosystem, Claiming it to be secured against the man-in-middle attack, Replay attack, and active and passive

attack using BAN logic. They simulated the technique uses AVISPA tool. This authentication scheme reduces the various cost overhead and time complexity. This authentication scheme reduces the various cost overhead and time complexity. It includes 5 phases are as follows.

Step-1: System Setup Phase

The server S selects two large primes p, q, where $p, q \equiv 3 \, mod \, 4$. The server S evaluates $N = p \times q$ and declares n as public key and (p, q) as private key.

Step-2: Registration Phase

Every new user needs to register with the server S to get the services/applications by executing the following steps:

- User U_i chooses random number R, identity ID_i and password PW_i He then computes $RPW_i = h\,(Id_i \| R \| PW_i)$ and submits $\{RPW_i, \ ID_i\}$ to the server S through a reliable channel.
- Upon obtaining the message from U_i, S generates a random nonce N_i and evaluates $MK = h\,(Id_i \| p \| q), Ai = MK \oplus h\,(RPW_i \| ID_i), CID_i = E\,h(p \| q)\,(ID_i \| N_i)\ and\ B_i = h\,(RPW_i \| MK)$. The server S stores the values $\{A_i, B_i, CID_i, n, h\,(.)\}$ into a smart card and transmits it to user U_i through a reliable channel.
- After getting the smart card from the server, U_i calculates $RN = h\,(ID_i \| PW_i) \oplus R\ and\ stores\ RN\ in\ the\ smart\ card$

Step-3: Login Phase

Whenever user U_i wants to access the services of remote server, he needs to log into the system by executing the following steps:

- U_i inserts smart card into a terminal and inputs $PW_i\ and\ ID_i$. The smart card evaluates $R' = h\,(ID_i \| PW_i) \oplus RN, RPW_i' = h\,(ID_i \| R' \| PW_i), MK' = A_i \oplus h\,(RPW_i' \| ID_i)$ and $B_i' = h\,(RPW_i' \| MK')$ and compares if $B_i = B_i'$. If it is false, the smart card aborts the session; otherwise, executes the next step.
- The smart card creates a random nonce R_c and evaluates $M_i = (Rc \| RPW_i \| ID_i)^2 \bmod n$, $J_i = h\,(R_c \| RPW_i \| ID_i)$, $L_i = J_i \oplus h\,(R_c \| ID_i)$ and $K_i = h\,(MK) \oplus R_c$. User U_i sends the message $\{M_i, L_i, K_i, CID_i\}$ to server over an insecure channel.

Step-3.1: Authentication and Key agreement phase

- After getting the message $\{M_i, L_i, K_i, \ CID_i\}$ from U_i, the server decrypts $CID_i, i.e.(ID_i \| N_i) = D_{h(p \| q)}(CID_i)\ and$ Checks the legitimacy of ID_i. If ID_i is not valid, server S aborts the session else it calculates $MK = h(ID_i \| p \| q), R_c' = h\,(MK) \oplus K_i\ and\ J_i' = L_i \oplus h\,(R_c \| ID_i)$.

- The server decrypts the message M_i with the help of private key *{p, q}* and obtains four root values $\{P_1, P_2, P_3, P_4\}. S\ checks\ if\ J_i' = h(P_k)$, where $k = 1\ to\ 4$. If it is false, S aborts the session; else, the server believes U_i is legal and performs next step.
- The server produces a random nonce R_s and calculates $T_i = h\,(R_s \| MK), CID_i^{\,n} = E_{h\,(p\,\|\,q)}\,(ID_i \| R_s)\,and\ R_{sc} = R_s \oplus R_c$. Server transmits $\{R_{sc}, T_i, CID_i^{\,n}\}\ to\ user\ U_i$ over an untrustworthy channel.
- Upon obtaining the reply message $\{R_{sc}, T_i, CID_i^{\,n}\}\ from\ S$, the smart $card$ calculates $R_s' = R_{sc} \oplus R_c$, $T_i' = h\,(R_s' \| MK)\ and$ checks if $T_i' = T_i$. If it holds, the user U_i trusts the server as legitimate one. User calculates the session key $SK = h\,(R_s \| R_c \| MK \| ID_i)\ and\ Z_i = h(SK \| ID_i)$. The user transmits Z_i to S and replaces $CID_i\ with\ CID_i^{\,n}$ in smart card.
- After receiving Z_i from U_i, the server enumerates $SK = h\,(R_s \| R_c \| MK \| ID_i)$, $Z_i' = h(SK \| ID_i)$ and checks $if\ Z_i = Z_i'$. If it is true, both parties can communicate using this session key SK.

Step-4: Password Change Phase

- The smart card reader checks the legitimacy of user U_i by performing the Step 1 of login phase.
- The user inputs a new password PW_i^{new} and calculates $RPW_i^{\,new} = h\,(ID_i \| R' \| PW_i^{\,new})$, $A_i^{new} = A_i \oplus h\,(RPW_i \| ID_i) \oplus h\,(RPW_i^{\,new} \| ID_i), B_i^{new} = h(RPW_i^{\,new} \| A_i \oplus h\,(RPW_i \| ID_i)$ and $RN^{new} = RN \oplus h\,(ID_i \| PW_i) \oplus h\,(ID_i \| PW_i^{\,new})$.
- The smart card reader stores new values $\{A_i^{new}, B_i^{new}, RN^{new}\}$ in place of old values $\{A_i, B_i, RN\}$ in the smart card. The password update phase is successfully completed.

(Dong, et.al. 2017) modified Rabin's cryptosystem using cubic residue technique which successfully removed the long cherished inconsistency so called four to one function in Rabin's cryptosystem. But, it was insecure against chosen cipher text attack that was pointed out by authors. Interestingly, the novel method of computing cubic root from a cubic residue prohibited the revealing private key. It is a modification of the Rabin Cryptosystem based on cubic residues Definition 1. If there exists an integer x such that $x^3 \equiv \alpha\ mod\ N, where\ \alpha \in Z\ and\ (\alpha, N) = 1$, α is called a cubic residue modulo N. Lemma 1: Suppose that p is a prime and $3 \mid (p-1)$, then α is a cubic residue modulo p iff $\alpha^{\frac{(p-1)}{3}} \equiv 1\ (mod\ p)$.

`Lemma 2:` Let P ≡ 2 (mod 3) and q ≡ 4 (mod 9) or 7 (mod 9) be primes, $N = p * q$. Then α is a cubic residue modulo $N = p * q$ if and only if α is a cubic residue modulo q. When constructing a quadratic residue y modulo $N = p * q$, y should be a quadratic residue both modulo p and modulo q. However, choosing proper p and q make easier to construct a cubic residue modulo $N = p * q$ than to construct a quadratic residue modulo $N = p * q$ by Lemma 2.

`Theorem 1:` Let, P ≡ 2 (mod 3) and q ≡ 4 (mod 9) or 7 (mod 9) be primes, $N = p * q$ and δ a cubic residue

modulo N. Then $\delta^{3d} \equiv \delta \pmod N$ where $d = \frac{\{2(p-1)(q-1)+3\}}{9}$, if q ≡ 4 (mod 9) and $d = \frac{\{(p-1)(q-1)+3\}}{9}$ if q ≡ 7 (mod 9). A $3^l\ th$ root of δ could be efficiently computed as mod $\tau \equiv \delta^{d^l}\ (mod\ N)$.

Algorithm for Key Setup:

Alice performs the following steps in order to get her private key and public key:

- choose two random prime numbers p and q such that P ≡ 2(mod 3) and q ≡ 4 (mod 9) or 7(mod 9) and p ⋣ q;
- Compute $N = p * q$,
- Publicize N as her public key, and keep (p, q) as her private key.

Algorithm for Encryption:

The sender Bob computes ciphertext (c) = m^3 (mod N) in order to send a confidential message m to Alice.

Algorithm for Decryption: Alice computes c^d (mod N) in order to decrypt the $ciphertext$ c, where $d = \frac{2(p-1)(q-1)+3}{9}$, If q ≡ 4 (mod 9) and d= $\frac{(p-1)(q-1)+3}{9}$ if q ≡ 7(mod 9). In fact, $c^d \equiv m^{3d} \equiv m\ (mod\ N)$ by Theorem 1.

A workout Example: Alice chooses prime numbers $p = 41\ and\ q = 31$, then computes $1271 = p * q = N$ is her public key, and $(p, q) = (41, 31)$ is her private key. Suppose that Bob send a confidential message $m = 1000$ to Alice. He computes $ciphertext\ c = 1000^3\ (mod\ 1271) = 78$. After receiving the $ciphertext$ c= 78, Alice computes $d = \frac{2(p-1)(q-1)+3}{9} = 267$, $c^d = 78^{267} \equiv 78^{40*6+27} \equiv 16 \bmod (41)$, and $78^{267} \equiv 8\ (mod\ 31)$. Then she uses the CRT to get the plaintext that is $m = 16 * 4 * 31 - 8 * 3 * 41 = 1000\ since\ 1 = 4 * 31 - 3 * 41$.

(Awad, et.al. 2018) proposed a deterministic method depending on the domain of Gaussian Integer to select right plaintext among four decryptions result. Recipient can decide particular plain text form four possible decryption result by selecting obtained square root with redundancies in its imaginary part (a + bi). This is the main benefit of using Gaussian integer technique. The disadvantage, on the other hand, same cyphertext can be generated from different plaintext due to having modular reduction arithmetic. For example, for the four plaintext $(m) = \{13, 20, 57, 64\}$, the same cipher text c=15.

The following algorithm is for computing the Gaussian square roots of the Gaussian quadratic residues modulo p.

Algorithm for computing the square roots modulo Gaussian Primes:

There are two possible forms for the message m ∈ A (N). The first form is $m = a + b_i$ where $a, b \in Z\ with\ b \neq 0$, while the second form is $m = a\ where\ a \in Z$ which is similar to that in the domain of natural integers. In this modification, the first case was considered when $m = a + b_i$ with b ≠ 0. To find the Gaussian square roots of the Gaussian quadratic residues $c = x + y_i$ in A (p) is not any easy problem although it could be solved by

generalizing the algorithms used to find square roots from Z_N *to* $Z[i]$. The following algorithm for computing the Gaussian square roots of the Gaussian quadratic residues modulo p.

Step-1: $\left(\frac{c}{p}\right) = -1$, if c is not quadratic residue modulo p.

Step-2: Compute the inverse $c^{-1}\ (mod\ p)$ by the e-Euclidean algorithm in $Z[i]$.

Step-3: Write $\varphi\ (p)\ = 2^s t$ where t is an odd integer.

Step-4: Select a quadratic non residue integer $b = x^l + {y_i}^l$ modulo $p\ \exists\, b \in\ R\ (p)$.

Step-5: $Set\ x\ \equiv\ b'(mod\ p)\ and\ r\ \equiv\ c^{\frac{(t+1)}{2}}\ (mod\ p)$.

Step-6: For i = 1 … … … … … … … $s - 1$

- Compute $\delta\ \equiv\ (r^2 * c^{-1})^{2s-i-1}\ (mod\ p)$.
- If$\delta\ \equiv\ -1\ (mod\ p) then\ set\ r\ \equiv\ r * x\ (mod\ p), and\ x \equiv\ x^2 (mod\ p)$.
- If $\delta\ \equiv\ 1(mod\ p), then\ repeat\ with\ a\ new\ value\ of\ i$.

Step-7: $Return\ (r, -r)\ as\ the\ two\ square\ roots\ of\ c\ modulo\ p$.

`Public and private keys generation algorithm:`

- Generate two large random and distinct Gaussian primes p and q, each roughly the same size and of the form $4k\ + 3$.
- Compute $N\ =\ p * q$.
- The public-key is N and A^{l}s private-key is (p, q).

`Messages Encryption Algorithm:`

- Obtain A's authentic public-key N, and choose the plaintext message as a Gaussian integer m ∈ A (N).
- Compute $the\ ciphertext\ c\ \equiv\ m^2\ (mod\ N)$, and send it to entity A.

`Ciphertext Decryption Algorithm:`

- Use the Chinese Remainder Theorem to find the four square roots m_1, m_2, m_3, and m_4 of c modulo N.
- Entity A decides which of these the original message m is by selecting the obtained square root with redundancies in its imaginary part.

`A workout example:` Let $p\ =\ 1051\ and\ q\ =\ 1031$ be two randomly chosen Gaussian integers of the form $4k\ + 3$, then $N\ =\ 1083581$. The public-key is 1083581 and A's private-key is the pair integer $(1051, 1031)$. The number of different choices for the message m is equal to the order of the complete residue system modulo N, which is $|\ A\ (N)| = 1174147783561$, Let $m = 101011 + 111111i$, then the ciphertext is c= $m^2 \equiv 891018 + 486027i$ (mod 1083581). To decrypt the Cypher message, an entity A should uses the private keys p and q including above algorithm, and the $Chinese$ Remainder Theorem over Z[i] to find the four square roots:

$m_1 = 101011 + 111111\text{i},\ m_2 = 428923 + 461094\text{i},\ m_3 = 654658 + 622487\text{i}$, and

$$m_4 = 982570 + 972470\text{i}.$$

An entity A knows that the original message is m_1 by checking the redundancy of the imaginary part of obtaining four square roots where the only one of them whose imaginary part contains a redundancy is m_1.

(Bhatt, et.al. 2018) extended a deterministic technique adding duplicating bits at the beginning of plaintext before encryption. Added replicating bits reflected within one decrypted text among four possible plaintext. The annoying thing is other three false result that refers to time complexity and memory complicity.

`Key Generating Algorithm:`

Input: Let f be the f-bit-size of the secret parameter.

Output: The private key p_1, p_2 and the public key N.

- First select two random prime numbers $p_1\ and\ p_2$ such that $2^f < p_1,\ p_2 < 2^{f+1}$ and p_1, p_2 are in the form of $4k + 3$ where k is any positive integer.
- Calculate $N = p_1 \times p_2$
- Calculate two integers α_1, α_2 such that $\alpha_1 \times p_2 + \alpha_2 \times p_2 = 1$
- *Return the private key* (p_1, p_2) *and the public key* N.

`Deterministic Rabin Encryption Algorithm:`

Input: $Public\ key: N, Plaintext: m_1$

Output: $Ciphertext: c_1$

- Select integer $0 < m_1 < N\ such\ that\ \ GCD\ (m_1, N) = 1$
- Convert the message m_1 into binary form and pad the digit with the LSB
- Compute $c_1 \equiv (m_1)^2\ mod\ N$
- Return the ciphertext c_1.

For the decryption of the ciphertext, Deterministic Rabin cryptosystem is used. The input of this algorithm is ciphertext and key pair and output the original plaintext. The decryption takes more time compared to encryption because; we used Chinese Remainder Theorem to find all possible plaintext. CRT takes more time to find the solution of set of congruent equations.

`Deterministic Rabin Decryption Algorithm:`

Input: Private Key: (p_1, p_2), Ciphertext: c_1

Output: Plaintext: m_1

Step-1: Calculate $r_1 \equiv c_1^{\frac{(p_1+1)}{4}} \pmod{p_1}$

Step-2: Calculate $r_2 \equiv c_2^{\frac{(p_2+1)}{4}} \pmod{p_2}$

Step-3: Calculate $x_1 \equiv (a_1 \times p_1 \times r_2 + a_2 \times p_2 \times r_1) \bmod N$

Step-4: Calculate $x_2 \equiv (a_1 \times p_1 \times r_2 - a_2 \times p_2 \times r_1) \bmod N$

Step-5: Calculate $x_3 \equiv -x_2 \pmod{N}$

Step-6: Calculate $x_4 \equiv -x_1 \pmod{N}$

Step-7: Among x_1, x_2, x_3, x_4 return the message having redundancy that is our original plaintext.

A workout example:

A real example uses prime numbers from 512 to 1024 bits long, similar to that used in RSA. For understanding purpose, we have taken small values. Let p_1 and p_2 are prime numbers and m1 is message. The example of proposed scheme is as follows: Let $p_1 = 7, p_2 = 11$ and message $(m_1) = 3$, public key $N = p_1 \times p_2 = 7 \times 11 = 77$ and then calculate $(-3) \times 7 + 2 \times 11 = 1, a_1 = -3 \; and \; a_2 = 2$, since m_1 is two bit message, whose bits are replicated to give 4 bits, till the number 63. Range of message is from 1 to 76, so redundancy of this type will work. Plaintext in binary form is written as $(11)_2$ or $(3)_{10}$. This replication gives $(1111)_2$ or $(15)_{10}$. Ciphertext is $c_1 = (m_1)^2 \; mod \; 77 = 71$. The decryption process is as follows.

$r_1 = 71^2 \; mod \; 7 = 1 \; and \; r_2 = 71^3 \; mod \; 11 = 4$, finally

$x_1 = ((-3) \times 7 \times 4 + 2 \times 11 \times 1) \; mod \; 77 = 15$

$x_2 = ((-3) \times 7 \times 1 - 2 \times 11 \times 4) \; mod \; 77 = 29.$

Two square root among four square roots are x_1 and x_2, and the rest two are $x_3 = -x_1 \bmod 77 = 62$, $x_4 = -x_2 \bmod 77 = 48$, hence, four square roots in binary formats: $15_{10} = 1111_2$, $29_{10} = 11101_2$, $62_{10} = 111110_2$, $48_{10} = 110000_2$

The required redundancy is possible in 15_{10} only, so number returned by the Deterministic Rabin machine is 15_{10}. The redundant bits are 11_2 or 3_{10}, which is original plaintext message. Deterministic Rabin Cryptosystem is similar to Rabin Cryptosystem but only difference between them is that, in Rabin Cryptosystem, there are four answers from which any one of them is correct. Therefore, Rabin cryptosystem is non-deterministic. It produces four answer and can be ascertained the correct result by checking the redundancy of the answer in binary form or by using repeated binary pattern like $(11\ 11)_2$.

(Gani, 2019) performed study over Rabin and RSA Cryptosystem and provided insightful discussion. The computation speed of RSA and Rabin's Cryptosystem were roughly same. Both algorithm's security relied on prime integer factorization.

(Mahad, et.al. 2015) proposed an efficient method to overcome four to one mapping problem of Rabin cryptosystem by reducing the phase space of plaintext from $M \in \mathbb{Z}_{pq}$ *to* $M \in 2^{2n-2}, 2^{2n-1} \subset \mathbb{Z}_{pq}$ where $N = p * q$ is a product of 2 strong primes $p * q \in 2^{2n}, 2^{2n+2}$. They calculated public key $N = p^2 * q$ as like as Okamoto-*Uchiyama's* scheme in 1998 and Schmidt-Samoa 2006. Private Key $d = p * q$,

`Key generation:`

Input: The size n-bit of the prime numbers.

Output: A public key $N = p^2 * q$ and the private key $d = p * q$,

- Generating two random and distinct n-bit strong primes p and q satisfying $p \equiv 3 \, mod \, 4, 2^{2n} < p < 2^{2n+2}$, $q \equiv 3 \, mod \, 4, 2^{2n} < q < 2^{2n+2}$
- *Set* $N = p^2 * q$ *and* $d = p * q$.

`Encryption:`

Input: A public key $N = p^2 * q$ and the plaintext M

Output: *The ciphertext* C.

- Plaintext is an integer $M \in 2^{2n} - 2, 2^{2n-1} \subset \mathbb{Z}_{pq}$
- Compute $C \equiv M^2 \, (mod \, N)$

`Decryption:`

Input: the private key tuple (d, p, q) and the *ciphertext* C

Output: The plaintext M.

Step-1: Computation $V \equiv C \, (mod \, d)$.

Step-2: Solving square root of V via CRT utilizing the private key pair (p, q).

Step-3: Return 4 possible plaintext M_1, M_2, M_3 and M_4

Step-4: For $i = 1 \, to \, 4$ compute Wi $= \frac{C - M_i^2}{N}$

Step-5: Return the plaintext M_i which produces $W_i \in \mathbb{Z}$

Proof of correctness begin with the following lemma.

`Lemma 1:` Let public key $N = p^2 * q$ and $d = p * q$, Choose $x \in \mathbb{Z}_d$. If $y \equiv x^2 \, (mod \, N)$ and $V \equiv y \, (mod \, d)$, then $V \equiv x^2 \, (mod \, d)$ Proof of lemma 1:

$y = x^2 + Nk_1$ where $k_1 \in \mathbb{Z}$ ..... Equ. (19)

$v = y + dk_2$ where $k_2 \in \mathbb{Z}$ ..... Equ. (20)

From Equ.(19, 20), we can write an equation $v = x^2 + Nk_1 + dk_2$ and finally $v \equiv x^2 \bmod d$. `Proposition 2:` Let C be an integer representing a cipher text encrypted by the Rabin–RZ scheme. Then $C \equiv M^2 \pmod N$ has a unique solution for M.

`Proof of proposition 2:`

Let begin with the proof of correctness of the decryption procedure. Since $M \in \mathbb{Z}_d$, we will obtain all 4 roots of V by solving $V \equiv C\ (mod\ d)$ using the CRT and also by lemma 1, indeed $v \equiv M^2\ (mod\ d)$ Furthermore, since $M \in \mathbb{Z}_d$ and d < N, certainly one of the root is a solution for $C \equiv M^2\ (mod\ N)$. We now proceed to prove the uniqueness. We rewrite the congruence relation as the equation $C \equiv M^2 \pmod N$ as $C \equiv M^2 - N_t$ with $t \in \mathbb{Z}, M_1 \neq M_2\ and\ for\ i = 1,2\ \ M_i < 2^{2n-1}$. Then ${M_1}^2 - Nt_1 = {M_2}^2 - Nt_2$, using $N = p^2 * q$, this leads to ${M_1}^2 - {M_2}^2 = (t_1 - t_2)N$

Case 1: $t_1 - t_2|\ (M_1^2 - M_2^2)$. The probability that $t_1 - t_2|\ (M_1^2 - M_2^2)$ and not equal to zero is 2^{-n}. Conversely, the probability that $t_1 - t_2|\ (M_1^2 - M_2^2)$ and equal to zero is $1 - \frac{1}{2^n}$. Thus $M_1^2 = M_2^2$ is with the probability is $1 - \frac{1}{2^{2n}}$ and since $M \in 2^{2n-2}.\ 2^{2n-1}$. Then $M_1 = M_2$, hence the equation $C = M^2 - N_t$ has only one solution.

Case 2: $N|\ (M_1 + M_2)(M_1 - M_2)$. The condition that should be satisfied is either one of the following conditions.

$$pq\ |(M_1 \pm M_2) \quad p^2\ |(M_1 \pm M_2)$$

or

$$p\ |(M_1 \pm M_2) \quad q\ |(M_1 \pm M_2)$$

Observe that $p * q,\ p^2 > 2^{2n}\ while\ M_1 \pm M_2 < 2.2^{2n-1} = 2^{2n}$. This implies that either condition is not possible.

`A workout example:`

The scenario is an entity A will send its public key to other entity B. B will encrypt. A choses Prime p=100669, q=69859 and compute $N = p^2 * q = 707968400363899\ and\ d = 7032635671, Message\ M = 1439948310$

$519659206359828 \equiv 1439948310^2\ (mod\ 707968400363899)\ and$ Sends to A. A decrypts the message by computing 3691358296 ≡ 519659206359828 mod 7032635671 .Then A uses the CRT and its private key S to compute the four square roots of $3691358296\ modulo\ d$ those are

- M_1=3890433108, M_2=1439948310, M_3=5592687361, M_4=3142202563.

Then, to determine the correct message A computes $for\ i = 1\ to\ 4$:

$$W_i = \frac{C - M_i^2}{N} \ldots\ldots\ldots\ldots Equ(21)$$

In this example only M_2 produces $W \in \mathbb{Z}$.

(Srivastava, et.al. 2013) presented analysis of Michael O. Rabin cryptosystem with the help of Chinese Reminder Theorem. Also, redundancy schemes for decryptions technique was mentioned and some basic mathematical concepts was explained and finally compared with RSA cryptosystem in terms of security and efficiency. The following descriptions for redundancy.

Redundancy schemes for unique decryption:

To ensure that decryption returns the correct message it is necessary to have some redundancy in the message, or else to send some extra bits. We can use following four solutions to overcome this problem.

Redundancy in the message for Rabin: For example, insist that the least significant l bits (where l > 2 is some known parameter) of the binary string m are all ones. If l is big enough then it is unlikely that two different choices of square root would have the right pattern in the l bits. A message m is encoded as $x = 2^l m + (2^l - 1)$, and so the message space $is\ M_k = \{m: 1 \leq m < \frac{N}{2^l}, gcd(N, 2^l * m + (2^l - 1)) = 1\}$, alternatively, $M_k = \{0,1\}^{\kappa - l - 2}$. The ciphertext is $c = x^2\ (mod\ N)$. Decryption involves computing the foursquare roots of c. If none, or more than one, of the roots has all l least significant bits equal to one and so corresponds to an element of $M_k$then decryption fails (return ⊥). Otherwise the output the message $m = \left\lfloor \frac{x}{2^l} \right\rfloor$.

A workout example:

Public key= $N = p * q = 77$, Private Key p=7, Private Key q=11

Let message $m = 15_{10} = 1111_2$

Left most bit=$11_2 = 3_{10} > 2$ and Right most bit =$11_2 = 3_{10}$,

Encoding message $x = 2^l * m + (2^l - 1) = 2^3 * 15 + (2^3 - 1) = 127$

$$x^2 = 127^2\ mod\ 77 = 36 = c$$

Decryption involves computing the foursquare roots of c.

Computation of two square roots $S_{r1} = 36^{\frac{7+1}{4}}\ mod\ 7 = \pm 1$, $S_{r2} = 36^{\frac{11+1}{4}}\ mod\ 11 = \pm 5$

Calculating two $bezout's$ coefficient using extended Euclidean Algorithm that is $a = -3\ and\ b = 2$

Chinese Remainder theorem gives four roots (X_1, X_2, X_3, X_4) by combing private key and their coefficient with two square roots

$x_1 = (p * a * S_{r2} + q * b * S_{r1}) mod\ N = (7 * -3 * 5 + 11 * 2 * 1)\ mod\ 77 = 71_{10}$

$x_2 = (p * a * S_{r2} + q * b * S_{r1}) mod\ N = (7 * -3 * -5 + 11 * 2 * -1) mod\ 77 = 6_{10}$

$X_3 = (p * a * S_{r2} - q * b * S_{r1}) mod\ N = (7 * -3 * 5 - 11 * 2 * 1)\ mod\ 77 = 27_{10}$

$X_4 = (p * a * S_{r2} - q * b * S_{r1}) mod\ N = (7 * -3 * -5 - 11 * 2 * -1) mod\ 77 = 50_{10}$

$X_1 = 71_{10} = 71,35,17,8,4,2,1 = 1000111_2$

$X_2 = 6_{10} = 6,3,1 = 110_2$

$X_3 = 27_{10} = 27,13,6,3,1 = 11011_2$

$X_4 = 50_{10} = 50,25,12,6,3,1 = 110010_2$

If none, or more than one of the roots has all l least significant bits equal to one and so corresponds to an element of M_k then decryption fails (return ⊥). Otherwise the output the message $m = floor\left\lfloor\frac{127}{2^3}\right\rfloor = 15$ which is desired plaintext.

Rabin padding scheme:

Public key= $N = p * q = 77$, Private Key $p = 7$, Private Key $q = 11$, message $m = 5_{10} = 101_2$ by padding another 5_{10} the message extend to $m = 101101_2$ which is equivalent to 45_{10}

Encryption: $C=45^2 \bmod 77=23$

Decryption: Decryption involves computing the foursquare roots of c. Computation of two square roots.

$S_{r1} = 23^{\frac{7+1}{4}} mod\ 7 = \pm 4, \quad S_{r2} = 23^{\frac{11+1}{4}} mod\ 11 = \pm 1$

Calculating two bezout's coefficient using Extended Euclidean Algorithm that is a=-3 and b=2. Chinese Remainder theorem gives four roots(X_1, X_2, X_3, X_4) by combining private key and their coefficient with two square roots.

$X_1 = (p * a * S_{r2} + q * b * S_{r1}) mod\ N = (7 * -3 * 1 + 11 * 2 * 4)\ mod\ 77 = 67_{10}$

$X_2 = (p * a * S_{r2} + q * b * S_{r1}) mod\ N = (7 * -3 * -1 + 11 * 2 * -4) mod\ 77 = 10_{10}$

$X_3 = (p * a * S_{r2} - q * b * S_{r1}) mod\ N = (7 * -3 * 1 - 11 * 2 * 4)\ mod\ 77 = 45_{10}$

$X_4 = (p * a * S_{r2} - q * b * S_{r1}) mod\ N = (7 * -3 * -1 - 11 * 2 * -4) mod\ 77 = 32_{10}$

Find the replicating bit after decimal to binary conversation

$X_1 = 67_{10} = 67,33,16,8,4,2,1 = 1000011_2$

$X_2 = 10_{10} = 10,5,2,1 = 1010_2$

$X_3 = 45_{10} = 45,22,11,5,2,1 = 101101_2$

$X_4 = 32_{10} = 32,16,8,4,2,1 = 100000_2$

Only root X_3 showing replicating bit. To retrieve original message, we have to remove replicating bit and reveal message $m=5_{10}$

Extra bits for Rabin:

Send two extra bits of information to specify the square root. For example, one could send the value $b_2 = \left(\frac{m}{N}\right)$ of the Jacobi symbol (the set $\{-1, 1\}$ can be encoded as a bit under the map $x \to 7\ (x+1)/2)$, together with the least significant bit b_2 of the message. The cipher text space is now $C_k = \left(Z/_{NZ}\right)^* \times \{0,1\}^2$ and, for simplicity of exposition, $M_k = \left(Z/_{NZ}\right)^*$. These two bits allow unique decryption, since $\left(\frac{-1}{N}\right) = 1$, m and N-m have the same Jacobi symbol and if m is odd then N-m is even. Indeed during using the CRT to compute square roots then one computes $m_p\ and\ m_q$ such that $\left(\frac{m_p}{p}\right) = \left(\frac{m_q}{q}\right)$ =1. Then decryption using the bits b_1, b_2 is: If $b_1 = -1$ then the decryption is $\pm CRT\ (m_p, m_q)$ and if $b_1 = -1$ then solution is $\pm\ CRT\ (-m_p, m_q)$. This scheme is close to optimal in terms of cipher text expansion and decryption never fails. The drawbacks are that the cipher text contains some information about the message, and encryption involves computing the Jacobi symbol, which typically requires far more computational resources than the single squaring modulo N.

A workout example:

Public key= $N = p * q = 77$, Private Key p=7, Private Key q=11, message $m = 15$, Root selection bit

$b_1 =$ m mod $2 = 15(2) = 1$

Message identification bit $b_2 = \left(\frac{m}{N}\right) = \left(\frac{15}{77}\right) = \left(\frac{15}{7}\right)\left(\frac{15}{11}\right) = \left(\frac{1}{7}\right)\left(\frac{4}{11}\right)$

$$= 1^{\frac{7-1}{2}}\ mod\ 7 * \left(2^{\frac{11-1}{2}}\ mod\ 11\right)^2 = 1,$$

Encipher $c=15^2$ mod 77=71

Then decryption using the bits b_1, b_2 after computing the four square roots of c.

Computation of two square roots $S_{r1} = 71^{\frac{7+1}{4}}\ mod\ 7 = \pm 1$, $S_{r2} = 71^{\frac{11+1}{4}}\ mod\ 11 = \pm 4$

$\left(\frac{1}{7}\right) = 1$ and $\left(\frac{4}{11}\right) = \left(2^{\frac{11-1}{2}}\ mod\ 11\right)^2 = 1$.Therefore $\left(\frac{S_{r1}}{N}\right) = \left(\frac{S_{r2}}{N}\right) = 1$

Calculating two bezout's coefficient using Extended Euclidean Algorithm that is $a = -3\ and\ b = 2$. Chinese Remainder theorem gives four roots (X_1, X_2, X_3, X_4) by combing private key and their coefficient with two square roots

$x_1 = (p * a * S_{r2} + q * b * S_{r1}) mod\ N = (7 * -3 * 4 + 11 * 2 * 1)\ mod\ 77 = 15_{10}$

$X_2 = (p * a * S_{r2} + q * b * S_{r1}) mod\ N = (7 * -3 * -4 + 11 * 2 * -1) mod\ 77 = 62_{10}$

$X_3 = (p * a * S_{r2} - q * b * S_{r1}) mod\ N = (7 * -3 * 4 - 11 * 2 * 1)\ mod\ 77 = 48_{10}$

$X_4 = (p * a * S_{r2} - q * b * S_{r1}) mod\ N = (7 * -3 * -4 - 11 * 2 * -1) mod\ 77 = 29_{10}$

Now select two roots specified by bit $b_1 = \{X_1, X_4\} = \{15,29\}$

Now compute Jacobi symbol of both of them.

$$\left(\frac{15}{77}\right) = \left(\frac{15}{7}\right)\left(\frac{15}{11}\right) = \left(\frac{1}{7}\right)\left(\frac{4}{11}\right) = 1 * \left(2^{\frac{11-1}{2}} \, mod \, 11\right)^2 = 1 * (-1)^2 = 1$$

$$\left(\frac{29}{77}\right) = \left(\frac{29}{7}\right)\left(\frac{29}{11}\right) = \left(\frac{1}{7}\right)\left(\frac{7}{11}\right) = 1 * (-1) = -1$$

As we can see Jacobi symbol $\left(\frac{15}{77}\right)$ is equivalent to b_2. Therefore original message $m = 15$ is retrieved. Let $N = p * q \; where \; p, q \equiv 3 \; (mod \; 4)$ If p ≡ ±q (mod 8) then $(N^2) = -1$. Hence, for every $1 \leq x < N$ exactly one of $x, N - x, 2x, N - 2x$ is a square modulo N. Without loss of generality we therefore assume that p ≡ 3 (mod 8) and q ≡ 7 (mod 8). The integer N is called a Williams integer in this situation. Williams [629] suggests encoding a message $1 \leq m < N/8 - 1$ (alternatively, $m \in M_k = \{0,1\}^{k-5}$) as an integer x such that x is even and $\left(\frac{x}{N}\right) = 1$ (and so $x \; or \; -x \; is \; a \; square \; modulo \; N$) by

$$x = p(m) = \begin{cases} 4(2m+1) & iff \left(\frac{2m+1}{N}\right) = 1 \\ 2(2m+1) & iff \left(\frac{2m+1}{N}\right) = -1 \end{cases} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots Equ. (22)$$

The encryption of m is then $c = P(m)^2 \; (mod \; N)$. One has $C_k = (Z/NZ)^*$. To decrypt one computes square roots to obtain the unique even integer $1 < x < N$ such that $(\frac{x}{N}) = 1$ and $x^2 \equiv c \pmod N$. If $8 \mid x$ then decryption fails (return ⊥). Otherwise, return m = (x/2 − 1)/2 if x ≡ 2 (mod 4) and m = (x/4 − 1)/2 if x ≡ 0 (mod 4).Unlike the extra bits scheme, this does not reveal information about the cipher text. It is almost optimal from the point of view of cipher text expansion. But it still requires encrypter to compute a Jacobi symbol otherwise loses performance advantage of Rabin over RSA. The Rabin cryptosystem with the Williams padding is sometimes called the Rabin-Williams cryptosystem.

A workout example: Assume that $p_1 \equiv 3 \; (mod \; 8) \; and \; p_2 \equiv 7 \; (mod \; 8)$. The integer N is called a Williams integer in this situation. Hence $P_1 = 8k + 3 = 11$ where $K = 1 \ldots\ldots\ldots\ldots\ldots p_1 - 1$ and $p_2 = 8k + 7 = 23, N = p * q = 253, K = 1 \ldots p_2 - 1. Message \; m = 13$. Williams's suggesting encoded message space $1 \leq m < \frac{N}{8} - 1$ as an integer x such that x is even and $\left(\frac{x}{N}\right) = 1$ (and $so \; x \; or \; -x$ is a square modulo N) by

$$x = p(m) = \begin{cases} 4(2m+1) & iff \left(\frac{2m+1}{N}\right) = 1 \\ 2(2m+1) & iff \left(\frac{2m+1}{N}\right) = -1 \end{cases} \ldots\ldots\ldots\ldots\ldots\ldots Equ. (23)$$

$$\left(\frac{2m+1}{N}\right) = \left(\frac{2*13+1}{253}\right) = \left(\frac{27}{11}\right)\left(\frac{27}{23}\right) = \left(\frac{5}{11}\right)\left(\frac{4}{23}\right) = 5^{\frac{11-1}{2}} \, mod \, 11 * \left(4^{\frac{23-1}{2}} \, mod \, 23\right)^2 = 1$$

$$C = X = \mathrm{p(m)}^2 \mathrm{mod\ N} = 4(2 * 13 + 1) = (108)^2 mod \; 253 = 26$$

Decryption Process:

To decrypt, one has to compute square roots to obtain the unique even integer 1<x<N such that

$\left(\frac{x}{N}\right) = 1 \; and \; x^2 \equiv c \; (mod \; N)$.

Root $c_1 = C^{\frac{11+1}{4}} \; mod \; 11 = 9 \; and$ Root $c_2 = C^{\frac{23+1}{4}} \; mod \; 23 = 16$. Now find two Bezout's coefficient from Extended Euclidean algorithm prime $p_1, p_2 \; that \; is \; a = -2 \; and \; b = 1 \; and \; apply \; those \; to \; CRT$.

$x_1 = (11 * -2 * 16 + 23 * 1 * 9) mod \; 253 = 108$

$x_2 = 253 - 108 \; = 145$

$x_3 = (11 * -2 * 16 - 23 * 1 * 9) mod \; 253 = 200$

$x_4 = 253 - 200 = 53$

The Jacobi symbol has to be computed after selecting even roots X_1 and X_3 among four tuple is as follows-

$$\left(\frac{X_1}{N}\right) = \left(\frac{108}{253}\right) = \left(\frac{108}{11}\right)\left(\frac{108}{23}\right) = \left(\frac{9}{11}\right)\left(\frac{16}{23}\right) = \left(\frac{3^2}{11}\right)\left(\frac{4^2}{23}\right)$$

$$= \left(3^{\frac{11-1}{2}} \; mod \; 11\right)^2 * \left(4^{\frac{23-1}{2}} \; mod \; 23\right)^2 = 1$$

Since we achieve positive Jacobi symbol, we do not need to calculate other one.

If 8 | X_1 then decryption fails (return ⊥). Otherwise, return expected message

$m = (X_1/2 - 1)/2 \quad iff \; X_1 \equiv 2 \; (mod \; 4) \; and$

$m = (X_1/4 - 1)/2 \quad iff \; X_1 \equiv 0 \; (mod \; 4)$.

Since 108≡ 0 (mod 4). Message m = $\frac{\left(\frac{Y_1}{4}-1\right)}{2} = \frac{\left(\frac{108}{4}-1\right)}{2} = \frac{26}{2} = 13$ retrieved.

2.3 Michael O. Rabin Signature Scheme

The Rabin signature algorithm in Cryptography is a method of digital signature originally proposed by Michael O. Rabin in 1979. The Rabin signature algorithm was one of the first digital signature schemes proposed, and it is the only one that relates to the hardness of forgery directly to the problem of integer factorization. The Rabin signature algorithm is existentially unforgeable in the random oracle model assuming the integer factorization problem is intractable. The Rabin signature algorithm is also closely related to the Rabin Cryptosystem. The security of Rabin signature relies on difficulties of integer factorization.

Unique Signature Algorithm:

$H \; (m) \; \frac{p-1}{2} \; mod \; p \; = 1 \; and \; H \; (m) \; \frac{q-1}{2} \; mod \; q \; = \; 1$, where hash function H is collision resistant if it is hard to finds that hash to the same output. If H is a collision resistant hash function which does not mean that no collision

exists, simply that they are hard to find. The cryptographic hash function is any mathematical equation. Message m is being hashed (encrypted). The hash value 1 generates by using private key p and q. The same hash value from different hashed input is so called collision resistant.

The signature S is given by the following equation.

$$S = ((p^{q-2}\, H\,(m)\, \frac{q+1}{4}\ \ mod\ q)\, p\ +\ (q^{p-2}\, H\,(m)\, \frac{p+1}{4}\ \ mod\ p)\, q)\ mod\ (pq)$$

Verification by $H\,(m)\ = s^2\ mod\ N, where\ N\ =\ p * q.$ The signature can be verified by everyone as N is public key.

The workout example:

Assuming that p=7 and q=11 using 4k+3 prime formation. The public key N= $p * q =\ 77.$ The *hashed* message $H(m) = 20^2\ mod\ 77 = 15$ coming from 13^2 mod 77. Let us see collision resistant hash value $15\ \frac{7-1}{2}\ \ mod\ 7\ =\ 1\ and\ 15\ \frac{11-1}{2}\ \ mod\ 11\ =\ 1$ that is vulnerable in collision attack because a collision attack on cryptographic hash tries to find two inputs producing same Hash value.

Signature S= $((\ 7^{11-2} * 15^{\frac{11+1}{4}} \bmod 11) * 7 + (11^{7-2} * 15^{\frac{7+1}{4}} \bmod 7) * 11\ ) \bmod 77$

$$= (6 * 7\ +\ 2 * 11)\ mod\ 77 = 64\ so\ the\ signature\ is\ unique.$$

Signature verification: H (m) =s^2 mod 77=64^2 mod 77=15.

Since H((m)=H(m), the signature is valid and accepted by verifier.

Pairing Signature Algorithm-1:

It is insecure without hash function.

Key Generation:

- The signer S chooses two primes p, q and computes $n\ =\ p *\ q$. S chooses a random $b(\ 0 \le b < N\ )$
- The public key is (N, b).
- The private key is (p, q).

Signing:

- To sign a message m the signer S picks random padding U and calculates $(m * U) mod\ N\ and$ Solves the equation $x\ (\ x\ +\ b\ ) mod\ N\ =\ (\ m * U)\ mod\ N.$
- If there is no solution S picks a new pad U and tries again.
- Else the signature on m is the $pair\ (U, X)$

Verification:

Given a message m and a signature (U, X) the verifier V calculates the equality of $X(X + b) \bmod N$ and $(m * U) \bmod N$. if equality is found, the signature is accepted as valid.

`A workout example`: Assuming that Private keys are $p = 7 * q = 11$ using $4k + 3$ prime formation, public keys are $N = p * q = 77$ and $b = 2$. The m is the hash value of $H(x) = 13^2 \bmod 77 = 15$, Let random padding $u = 13, x = 13$ those are suited for the following equation. Attempts are continue until they are equal.

$x(x + b)\ mod\ N$	$M * U\ mod\ N$
$\Rightarrow 15\ (15 + 2)\ mod\ 77$	$\Rightarrow\ (15.17)\ mod\ 77$
$= 24$	$= 24$

The equation is solvable that is why the signature on m is the pair (17,15)

`Verification message:`

The verifier checks the equality by calculating $x(x + b)$ and $(m * U) \bmod N$. If $x(x + b) \bmod N = (m * U) \bmod N$, the signature $(17, 15)$ on m is valid and accepted.

`Pairing Signature Algorithm-2:`

It is secure with hash function. In most presentations in modern terminology the algorithm is simplified by choosing b = 0. The algorithm relies on a collision-resistant hash function $H: \{0,1\}^* \rightarrow \{0,1\}^k$. The hash function H with k output bits is assumed to be a random oracle (certain decision problem is solved by single operation) and the algorithm works as follows:

Key Generation:

- The signer S chooses primes p, q and computes the product $N = p * q$
- The public key is N.
- The private key is (p, q).

Signing:

- Signer S picks random padding U to sign a message m and calculates $H\ (m * U)\ mod\ N$. S then solves the equation $x^2 = H\ (m * U)\ mod\ N$.
- If there is no solution S picks a new pad U and try again.
- Else the signature on m is (U, X)

Verification:

Given a message m and a signature (U, X) the verifier V calculates equality of $x^2 \bmod N$ and $H(m * U) \bmod N$. If equality is found, the signature is accepted as valid.

A workout example:

Assuming that Alice wants send a secret information$(X = 20)$ to Bob using valid signature. She first hashes the secret by $m^2 \bmod N = 20^2 \bmod 77 = 15$ where N is a composite number of two secret private keys are moduli p=7, moduli q=11, both are Blum prime (4k+3). Public key or modulus $N = p * q = 7 * 11 = 77$. The hashed value 15 will be used to generate signature. Signing: $(15, 25, 12)$ to do that first signer S chooses number U probabilistically and see the value of random oracle modulo N matches any quadratic residue modulo N. This process continue until both sides of the equation match the hash. Let $U = 25$ for that $15 * 25 \bmod 77 = 67$ and now take such x value for which quadratic residue 67 can be obtained.

$m * U \bmod N = 15 * 25 \bmod 77 = 67$ | $X^2 \bmod N = 12^2 \bmod 77 = 67$

Now both sides are equal so the verifier accepts the signature as valid,

2.3.1 Existing Research on Michael O. Rabin Signature Scheme

Rabin signature of a message m may consist of single or $pair\ (m, S)$. However, if $x^2 = m\ mod\ N$ has no solution, this signature cannot be directly generated. To overcome this obstruction, a random pad U was proposed by (Pieprzyk, et.al. 2003) and attempts are repeated until $x^2 = (m * U)\ mod\ N$ is solvable and thus the signature is the triple (m, U, S). A verifier compares $m*U \bmod N$ with S^2 and accepts the signature as valid when these two numbers are equal. (Williams, 1980) devised a modification of the Rabin system which allows the cryptographer to decide definitively which of the four square roots the original message is. The security of Rabin-Williams's signature system rely on finding difficulties of square roots. But it did not offer multiple signature facilities in single document. It avoids the forgery vulnerability. While that scheme requires the use of two primes respectively congruent to 3 and 7 modulo 8. Moreover in the Rabin-Williams scheme, a message cannot be signed twice in two different ways, otherwise the factorization of N might get exposed. (Elia, et.al. 2011& 2012) presented a modification of H. C. William scheme based on the computation of a Jacobi symbol, where deterministic pad used for two purposes is as follows.

Signing using deterministic pad-1:

The following deterministic pad calculation method for non Blum prime when m is QNR. When m is not quadratic, we use Jacobi Symbol to compute suitable pad and obtain quadratic residues modulo p and q. The quadratic

equation $x^2 = m \, mod \, N$ is solvable if and only if m is a quadratic residue modulo N and that m is also quadratic residue modulo p and modulo q.

$$f_1 = \frac{m_1}{2}\left\{1 - \left(\frac{m_1}{p}\right)\right\} + \frac{1}{2}\left\{1 + \left(\frac{m_1}{p}\right)\right\} \ldots\ldots Equ(24)$$

$$f_2 = \frac{m_2}{2}\left\{1 - \left(\frac{m_2}{q}\right)\right\} + \frac{1}{2}\left\{1 + \left(\frac{m_2}{q}\right)\right\} \ldots\ldots Equ(25)$$

$$m = \{m_1\psi_1 + m_2\psi_2\} mod \, N \ldots\ldots\ldots\ldots Equ(26)$$

$x^2 = (m_1\psi_1 + m_2\psi_2)(f_1\psi_1 + f_2\psi_2) = (f_1 m_1\psi_1 + f_2 m_2\psi_2) \, mod \, N$, where $f_1 \, m_1 \, and \, f_2 \, m_2$ is a quadratic residue modulo p and modulo q respectively, since $\left(\frac{m_1}{p}\right) = \left(\frac{f_1}{p}\right)$, $\left(\frac{m_2}{q}\right) = \left(\frac{f_2}{q}\right)$ so that

$$\left(\frac{m_1 f_1}{p}\right) = \left(\frac{m_1}{p}\right)\left(\frac{f_1}{p}\right) = 1, \; \left(\frac{m_2 f_2}{q}\right) = \left(\frac{m_2}{q}\right)\left(\frac{f_2}{q}\right) = 1$$

$$U = R^2\{f_1\psi_1 + f_2\psi_2\} \ldots\ldots\ldots Equ(27)$$

A workout example: Assuming that Alice wants to send a secret information (x= 97) to Bob using valid signature. She first hashes the secret by $x^2 \, mod \, N = 97^2 \, mod \, 377 = 361$ where N is a composite number of two secret private keys that is moduli p=13, moduli q=29, public key or modulus $N = p * q = 13 * 29 = 377$. The hashed value 361 will be used to generate signature.

$m_1 = 361 \, mod \, 13 = 10, \; m_2 = 361 \, mod \, 29 = 13$

The Legendre symbol $\left(\frac{10}{13}\right)$ is quadratic residue $= +1$

1^2 mod 13=1, 2^2 mod 13= 4, 3^2 mod 13=9, 4^2 mod 13= 3, 5^2 mod 13=12, 6^2 mod 13=10, 7^2 mod 13=10, 8^2 mod 13=12, 9^2 mod 13=3, 10^2 mod 13=9. 11^2 mod 13=4, 12^2 mod 13=1. 13^2 mod 13=0 that is why calculation is done up to p-1. Hence, 10 over 13 is a quadratic residue under modulo 13 that exactly appears twice.

The Legendre symbol $\left(\frac{13}{29}\right)$ is quadratic non residue = -1

1^2 mod 29=1, 2^2 mod 29= 4, 3^2 mod 29=9, 4^2 mod 29= 3, 5^2 mod 29=12, 6^2 mod 29= 7, 7^2 mod 29=20, 8^2 mod 29=6, 9^2 mod 29=23, 10^2 mod 29=13. 11^2 mod 29=5, 12^2 mod 29=28, 13^2 mod 29=24, 14^2 mod 29=22, 15^2 mod 29= 22, 15^2 mod 29=24, 17^2 mod 29= 28, 18^2 mod 29=5, 19^2 mod 29=13,20^2 mod 29=23, 21^2 mod 29=6, 22^2 mod 29=20, 23^2 mod 29=7. 24^2 mod 29=25, 25^2 mod 29=16, 26^2 mod 29=9, 27^2 mod 29=4, 28^2 mod 29=1, 13 over 29 is a quadratic non residue under modulo 29 that exactly appears once. Now using *Equ.(24, 25, 26, 27)* the following signature generated mathematics is calculated.

$$f_1 = \frac{10}{2}\left\{1 - \left(\frac{10}{13}\right)\right\} + \frac{1}{2}\left\{1 + \left(\frac{10}{13}\right)\right\} = \frac{10}{2}\{1 - 1\} + \frac{1}{2}\{1 + 1\} = 11$$

$$f_2 = \frac{13}{2}\left\{1 - \left(\frac{13}{29}\right)\right\} + \frac{1}{2}\left\{1 + \left(\frac{13}{29}\right)\right\} = \frac{13}{2}\{1 - (-1)\} + \frac{1}{2}\{1 + (-1)\} = 13$$

$m = m_1\psi_1 + m_2\psi_2 \; mod\; N = 10 * 117 + 13 * (-116) \; mod\; 377$

$= -338(377) = 377 - 338 = 39$

$X^2 = (m_1\psi_1 + m_2\psi_2)(f_1\psi_1 + f_2\psi_2) = (f_1 m_1\psi_1 + f_2 m_2\psi_2) \; mod\; N$

$= 1 * 10 * 117 + 13 * 13 * (-116)$
$= -18434 \; mod\; 377$
$= (377 * 49) - 18434$
$= 18473 - 18434 = 39$

The deterministic padding factor is as follows.

$U = R^2\{f_1\psi_1 + f_2\psi_2\} = 1^2\{1 * 117 + 13(-116)\} \; mod\; 377$

$= -1391(377) = (377 * 4) - 1391 = 1508 - 1391 = 117.$

S is the solution of the equation $x^2 = (m * U) \; mod\; N = 39 * 17\,(377) = 39$

Signed message: $(39, 117, 39)$

Verification:

The Signer S verify the equation $x^2 = (m * U) \bmod N = 39 * 117\,(377) = 39$. Since L. H. S (39) = R. H. S (39), so the signature is valid for message 97. This is deterministically true as X^2 pre-calculated but probabilistically there is no such x value for which the $x^2 = (m * U) \bmod N$ is true.

`Signing using deterministic pad-2`: The followings are deterministically pad calculation method for Blum prime (4k+3) when m is QNR.

$f_1 = \left(\frac{m_1}{p}\right) \ldots\ldots Equ(28)$, $f_2 = \left(\frac{m_2}{q}\right) \ldots\ldots\ldots\ldots Equ(29)$

$m = \{m_1\psi_1 + m_2\psi_2\} mod\; N \ldots\ldots\ldots\ldots Equ(30)$

$x^2 = (m_1\psi_1 + m_2\psi_2)(f_1\psi_1 + f_2\psi_2) = (f_1 m_1\psi_1 + f_2 m_2\psi_2) \quad mod\; N$, where $f_1\, m_1\; and\; f_2\, m_2$ is a quadratic residue modulo p and modulo q respectively, since $\left(\frac{m_1}{p}\right) = \left(\frac{f_1}{p}\right)$, $\left(\frac{m_2}{q}\right) = \left(\frac{f_2}{q}\right)$ so that $\left(\frac{m_1 f_1}{p}\right) = \left(\frac{m_1}{p}\right)\left(\frac{f_1}{p}\right) = 1$, $\left(\frac{m_2 f_2}{q}\right) = \left(\frac{m_2}{q}\right)\left(\frac{f_2}{q}\right) = 1$, $U = R^2\{f_1\psi_1 + f_2\psi_2\} \ldots\ldots\ldots\ldots Equ(31)$

S is the solution of the equation $x^2 = (m * U) \; mod\; N$

Signed message: $\{m, U, S\}$

Verification: equation $s^2 = (m * U) \; mod\; N$, the signature is valid if and only if equation is true.

A workout Example: Assuming that Alice wants to send a secret information (x=20) to Bob using valid signature. She first hashes the secret by $X^2\ mod\ N = 20^2\ mod\ 77 = 15$ where N is a composite number of two secret private keys those are moduli p=7, moduli q=11, public key or modulus $N = p * q = 7 * 11 = 77$. The hashed value 15 will be used to generate signature. Now using *Equ.(28, 29, 30, 31*), the following problem has been solved.

$m_1 = 15 \bmod 7 = 1, m_2 = 15 \bmod 11 = 4, f_1 = \left(\frac{1}{7}\right) = 1,$

First let's check whether 1 over 7 is a quadratic residue or not? For that purposes, we have to check from 1 to p-1. 1^2 mod 7=1, 2^2 mod 7= 4, 3^2 mod 7=2, 4^2 mod 7= 2, 5^2 mod 7= 4, 6^2 mod 7= 1. It's clear that 1 over 7 is a quadratic residue modulo 7.

$f_2 = \left(\frac{4}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{2}{11}\right) = (-1)(-1) = 1$, According to Legendre symbol first let's check whether 2 over 11 is a quadratic residue or not? For that purposes, we have to check from 1 to p-1. 1^2 mod 11=1, 2^2 mod 11= 4, 3^2 mod 11=9, 4^2 mod 11= 5, 5^2 mod 11= 3, 6^2 mod 11= 3, 7^2 mod 11=5, 8^2 mod 11= 9, 9^2 mod 11=4, 10^2 mod 11= 1. It's clear that 2 over 11 is not a quadratic residue modulo 11.

$m = m_1\psi_1 + m_2\psi_2\ mod\ N = 1 * 22 + 4(-21)\ mod\ 77 = 15$

$x^2 = (m_1\psi_1 + m_2\psi_2)(f_1\psi_1 + f_2\psi_2) = (f_1 m_1\psi_1 + f_2 m_2\psi_2)\ mod\ N$

$= \{1 * 1 * 22 + 1 * 4 * (-21)\}mod\ 77 = 15$

$U = R^2\{f_1\psi_1 + f_2\psi_2\} = 1^2\{1 * 22 + 1 * (-21)\} = 1$, Choose such R value for which m*U mod N equal to x^2(pre-calculated).

Signed message: $\{15, 1\ and\ 15\}$ where S is the solution of the equation $x^2 = (m * U)\ mod\ N$. In this circumstances we do not need to find such x value to solve the equation $x^2 = (m * U)\ mod\ N$ as this method is deterministic. But it was needed to find such X value if it would be probabilistic. Verification: equation $s^2 = (m * U)\ mod\ N$., the signature is valid if and only if the equation is true. $= 15 * 1\ mod\ 77 = 15$, $S^2\ equivalent\ to\ X^2$ which value 15 is already computed. Since $L.H.S = R.H.S$, Hence the signature is accepted as valid.

Using a deterministic pad as above, allows different signatures of the same document. It is vulnerable to forgery attacks. It is relatively easy to compute S^2 mod N, choose any message m' and compute multiplicative inverse of m' (hash value of m), compute $U' = S^2 * m'^{-1}\ mod\ N$ and forge the signature as (m'^{-1}, U', s) without knowing the factorization of N. The following variant countering the forgery attack or vulnerability of Rabin's signature.

Signed Message: $(m, U * R^2 \ mod\ N, S * R^3 \ mod\ N, R^4 \ mod\ N)$, so the signature is four tuple where U is padding factor and R is a random number selection, Here S is the x's value for which equation $x^2 = (m * U) \ mod\ N \ is\ true$. It is clearly seen that x and U both unknown number which has to be chosen by entity A in order to generate signature.

Verification: Verifier computes $(S * K^3)^2 \ mod\ N$ and $(m * U * R^2 * R^4) \ mod\ N$ and accept the signature is valid if and only if aforesaid two number is equal.

A workout example: Assuming preprocessed $m' = 15, U * R^2 = 25 * 3^2 \ mod\ 77 = 71,\ S * R^2 = 12 * 3^2 = 108 \ mod\ 77 = 48 \ and\ 3^4 \ mod\ 77 = 4$. So the signature (15, 71, 48, and 4) is four tuple. The verification computations is as follows

- $(12*3^3)^2$ mod 77= (12^2*3^6) mod 77= 25 and
- $15*25*3^2*3^4$ mod 77=25

Counter forgery 4-tuple signature (15, 71, 48, and 41) verification is successful, so the signature is valid and accepted

(Elia, et.al, 2013) Described also a crypto intensive technique on Rabin cryptosystem based on Group isomorphism. It is in combination of Homomorphism and $bijection$. A possible solution is to use a function ∂ defined from Z_N into a group G of the same order, and define a function ∂_1 such that ∂_1 $(x_1) = \partial(x_2)$. The public key consists of the two functions ∂ and ∂_1. At the encryption stage, both are evaluated at the same argument, the message m and the minimum information necessary to distinguish their values is delivered together with the encrypted message. The decryption operations are obvious. The true limitation of this scheme is that ∂ must be a one-way function, otherwise two square roots that allow us to factor N can be recovered as in the residuosity subsection. This approach come to exits that given N, let $P = \mu^N + 1$ computes smallest prime using Mobius function that certainly exists by $Dirichlet's$ theorem (Apostol, 1976) that is congruent 1 modulo N. Let g be a primitive element generating the multiplicative group Z^*_P.

Define $g_1 = g^{\mu}$ and $g_2 = g^{\mu(\psi_1 - \psi_2)}$, and as usual let m denote the message.

Public key: {N, P, g_1, g_2}

Encryption stage: C, b_0, d_1, d_2, p_1, p_2} where $C = m^2 \bmod N, b_0 = m \bmod 2$, p_1 is a position in the binary expansion of $g_1{}^m \bmod p$, whose bit d_1 is different from the bit in the corresponding position of the binary expansion of $g_2{}^m \bmod p$, and p_2 is a positioning the binary expansion of $g_1{}^m \bmod p$, whose bit d_2 is different from the bit in the corresponding position of the binary expansion of $g_2{}^{-m} \ mod\ p$.

Decryption stage:

- compute, as in (3), the four roots, written as positive numbers,
- take the two roots having the same parity specified by b_0, say z_1 and z_2,
- Compute A = $g_1^{z_1} \bmod p$ and B $= g_1^{z_2} \bmod p$
- Between z_1 and z_2, the root is selected that has the correct bits d_1 and d_2 in both the given positions p_1 and p_2 of the binary expansion of A or B.The algorithm is justified by the following Lemma.

Lemma 6. The power $g_0 = g^{\mu}$ generates a group of order N in Z_p^*, thus the correspondence $x \leftrightarrow g_0^x$ establishes an isomorphism between a multiplicative subgroup of Z_p^* and the additive group of Z_N^*.

A workout example:

An isomorphism (Homomorphism + bijection) establishes a mathematical mapping or operation between multiplicative subgroup of integer Z_p and additive group of integer Z_N^*. These are multiplicative subgroup G^*_7 and G^*_{11} what have been introduced in appendix C. It is being seen that each row is permutation of other row except first row. Simply we can say two mathematical objects are isomorphic if an isomorphism exists among them. The additive group of composite number has been shown in appendix C.

According to pre-definition, Let $p = 7, q = 11, N = 77, P = \mu^N + 1 = \mu^{(7*11)} + 1$

$= (-1)^2 + 1 = 2$, 1st Generator of group $g_1 = g^{\mu}$ *and* 1st Generator of group $g_2 = g^{\mu(22+21)} = g^{\mu(43)} = g^{-1}$ and $m = 13$ denoted the message.

Public key: $\{77, 2, g_1, g_2\}$.

Encryption stage: {C, b_0, d_1, d_2, p_1, p_2}, where C = 13^2 mod 77=15, b_0 = 13 mod 2=1,

$P_1 = g_1^m \bmod P = 3^{13} \bmod 2 = 1$, $d_1 = g_2^m \bmod P = (3^{-1})^{13} \bmod 2 = 1$.

$P_2 = g_1^m \bmod P = {}_2{}^{13} \bmod 2 = 0$, $d_2 = g_2^{-m} \bmod P = (3^{-1})^{-13} \bmod 2 = 3^{13} \bmod 2 = 1$

Decryption stage: Step (1, 2) is expressed by congruence law .

Step-1: $\frac{77}{7}$ $V_1 \equiv 1 \bmod 7 \rightarrow 11\ V_1 \equiv 1 \bmod 7 \rightarrow 2\ V_1 \equiv 1 \bmod 7 \rightarrow V_1 = 2$

Step-2: $\frac{77}{11}$ $V_2 \equiv 1 \bmod 11 \rightarrow 7\ V_2 \equiv 1 \bmod 11 \rightarrow (-3)V_2 \equiv 1 \bmod 11 \rightarrow V_1 = 8$

The following roots are deterministic polynomial time for Blum prime.

$$a_1 = C^{\left(\frac{p+1}{4}\right)} \bmod p = 15^2 \bmod 7 = 1$$

$$a_2 = C^{\left(\frac{q+1}{4}\right)} \bmod q = 15^3 \bmod 7 = 9$$

[+ +]

$$a_3 = p - a_1 = 7 - 1 = 6 \ (inverse\ of\ a_1)$$

$$a_4 = q - a_2 = 11 - 9 = 2 \ (inverse\ of\ a_2)$$

[- -]

Now according to CRT, Four roots are calculated as follows.

Step-1: [+ +] $Z \equiv 1 \bmod 7$ and $Z \equiv 9 \bmod 11$

$$Z_1 = \left\{a_1 * V_1 * \frac{N}{p} + a_2 * V_2 * \frac{N}{q}\right\} \bmod N$$

$$= \left\{1 * 2 * \frac{77}{7} + 9 * 8 * \frac{77}{11}\right\} \bmod 77 = 527 \bmod 77 = 64$$

Step-2: [- -] $Z \equiv 6 \bmod 7$ and $Z \equiv 2 \bmod 11$

$$Z_2 = \left\{a_3 * V_1 * \frac{N}{p} + a_4 * V_2 * \frac{N}{q}\right\} \bmod N$$

$$= \left\{6 * 2 * \frac{77}{7} + 2 * 8 * \frac{77}{11}\right\} \bmod 77 = 244 \bmod 77 = 13$$

Step-3: [+ -] $Z \equiv 1 \bmod 7$ and $Z \equiv 2 \bmod 11$

$$Z_3 = \left\{a_1 * V_1 * \frac{N}{p} + a_4 * V_2 * \frac{N}{q}\right\} \bmod N$$

$$= \left\{1 * 2 * \frac{77}{7} + 2 * 8 * \frac{77}{11}\right\} \bmod 77 = 134 \bmod 77 = 57$$

Step-4: [- +] $Z \equiv 6 \bmod 7$ and $Z \equiv 9 \bmod 11$

$$Z_4 = \left\{a_2 * V_1 * \frac{N}{p} + a_3 * V_2 * \frac{N}{q}\right\} \bmod N$$

$$= \left\{6 * 2 * \frac{77}{7} + 9 * 8 * \frac{77}{11}\right\} \bmod 77 = 636 \bmod 77 = 20$$

Choose two roots specified by b_0 and rearrangement them as first small root for small group and larger root for larger group. Those are $(Z_2, Z_3) = (13, 57)$.

Computations:

$A = {g_1}^{z_2} \bmod P$, $A = 3^{z_2} \bmod P = 3^{13}\ mod\ 2 = 1$ (this is for small group)

$B = {g_1}^{z_3} \bmod P = 2^{57} \bmod 2 = (2^8)^7 * 2^1\ mod\ 2 = 0$ (this for larger group). It is clearly seen that A matches to d_1 since P_1 and d_1 are one to one correspondence. Hence, Z_2=13 is our plaintext.

(Sidorov,et.al., 2015) described a bug into implementation of Rabin-Williams digital signature in crypto++ framework which is a popular cryptographic framework. The bug is the misuse of blinding technique that is aimed at preventing timing attack on the digital signature system implementation. To fix the *bugdoors* one should ensure that the value used for blinding is a quadratic residue modulo p and q. This conditions guarantees that the blinding value will be removed at the unbinding step and won't affect the result of the signing procedure. Although the authors of crypto++ aimed at improving the security of the Rabin-Williams signature system implementation but eventually made the system completely insecure admitted by authors themselves. The Rabin-Williams signatures

become more efficient from state-of-the-art modular –root signature system which was far beyond the simple signature system introduced by (Bernstein, 2008).

(Jaweria, et.al. 2017) proposed a secure gateway discovery protocol using Rabin Signature Scheme in MANET that ensures confidentiality goal in heterogeneous environments. Registration process was included to remove the malicious nodes. This protocol removes the threat of anti-confidentiality, anti-authentication and anti-duplication. The efficiency of this protocol is shown through AVISPA tool.

(Chaoyang, et, al.,2017) proposed an efficient ID-based signature scheme based on Rabin's cryptosystem by using the forking lemma theorem. This scheme has less exponential operations, it is secure against existential forgery under adaptively chosen identity and message attacks in the random oracle model.

(Bleichenbacher, 2004)] presented a method to compress Rabin signature. Rabin signatures and compressed signatures are equally difficult to forge. Compression requires a continued fraction expansion and takes time $O(log(n)_2)$. Decompression requires two multiplications and an inverse over $\mathbb{Z}\,\mathbb{Z}/_n\mathbb{Z}\,\mathbb{Z}$ and a square root in $\mathbb{Z}\,\mathbb{Z}$ and require time $O(log(n)_2$.

2.4 Key distribution protocol

(Stalling,W., 2016) presented Diffie– Hellman key exchange protocol which was introduced by Malcolm John Williamson (British mathematician and cryptographer) in 1976. The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography. It is generally referred to as Diffie-Hellman key exchange protocol. A number of commercial products employ this key exchange technique. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption and decryption of messages. The algorithm itself is limited to the exchange of secret values. The security of Diffie-Hellman algorithm depends on the difficulty of computing discrete logarithms.

Global Public elements: N is a prime number which can define a domain so called curve area or elliptic curve, α is a primitive root of N such that $\alpha < N$.

Key Generation for user A: Select private key Xa such that $Xa < N$ and then

calculate public key $Ya = \alpha^{xa} \ mod \ N$.

Key Generation for user B: Select private key X_b such that $X_b < N$ and then

calculate public key $Y_b = \alpha^{xb} \ mod \ N$

Secret key for user A : $K = (Y_b)^{xa} \ mod \ N$

Secret key for user B : $K = (Y_a)^{xb} \ mod \ N$

A workout Example:

An integer number N = 353 that is domain size and its primitive root α = 3. A and B select secret keys A = 97 and B = 233, respectively. Each of them computes public key:

A computes $X = 3^{97} \bmod 353 = 40$ and B computes $Y = 3^{233} \bmod 353 = 248$.

They compute secret key in the following ways by exchanging public key between each other. A computes $K = (Y)^A \ mod \ 353 = 24897 \ \ mod \ 353 = 160$ and B computes $K = (X)^B \ mod \ 353 = 40233 \ mod \ 353 = 160$.

2.4.1 Brute-force Attack

We assume an attacker would have available the following public information:

N = 353, α = 3, $Y_A = 40$, $Y_B = 248$. It would be possible by brute-force to determine the secret key 160. In particular, an attacker Eve can determine the common key by discovering a solution to the following equations:

$3^a \ mod \ 353 = 40$……*Equ.(32)*

$3^b \ mod \ 353 = 248$……..……*Equ(33)*

The brute-force approach is to calculate exponentiations of 3 modulo 353, stopping when the result equals either 40 or 248. The desired answer is reached with the indices of 97 which provides $3^{97} \bmod 353 = 40$. However, with the larger numbers, the problem becomes impractical.

2.4.2 The Man-in-the middle attack

The protocol is insecure against man-in-the-middle attack. Suppose Alice and Bob wish to exchange keys and Darth is the adversary. The attack proceeds as follows.

Step-1: Darth prepares for the attack by generating two random private keys X_{D_1} and

X_{D_2} and then computing the corresponding public keys Y_{D_1} and Y_{D_2}

Step-2: Alice transmits Y_A to Bob.

Step-3: Darth intercepts Y_A and transmits Y_{D_1} to Bob. Darth also computes

$$K_2 = (Y_A)^{X_{D_2}} \, mod \, N$$

Step-4: Bob receives Y_{D_1} and calculates $K_1 = (Y_{D_1})^{X_B} \, mod \, N$

Step-5: Bob transmit Y_B to Alice.

Step-6: Darth intercepts Y_B and transmits Y_{D_2} to Alice. She computes also

$$K_1 = (Y_B)^{X_{D_1}} \, mod \, N$$

Step-7: Alice receives Y_{D_2} and calculates $K_2 = (Y_{D_2})^{X_A} \, mod \, N$

A workout example:

Table 2.4: The process of the man-in-the-middle attack

 Alice	 Darth	 Bob
Private Key X_A=2 public key $Y_A = \alpha^{X_A} \, mod \, N$  =9	Private keys $X_{D_1} = 7$, $X_{D_2} = 11$, Public keys: $Y_{D_1} = \alpha^{X_{D_1}} \bmod N = 69$ $Y_{D_2} = \alpha^{X_{D_2}} \bmod N = 294$ Y_{D_1} Intercepting key = 9, Calculating secret key $K_2 = (Y_A)^{X_{D_2}} mod \, N = 304$	Private key X_B = 5 and public key $Y_B = \alpha^{X_B} \, mod \, N$=243 Calculating secret key $K_1 = (Y_{D_1})^{X_B} mod \, N = 250$
Secret key $K_2 = (Y_{D_2})^{X_A} \, mod \, N = 304$ Alice and Darth shared secret key K_2	Y_{D_2}  Calculating secret key $K_1 = (Y_B)^{X_{D_1}} mod \, N = 250$	 Y_B Bob and Darth shared secret key K_1

At this point Bob and Alice think that they share a secret key but instead Bob and Darth share secret key K_1 and Alice and Darth share secret key K_2.

All further communication between Bob and Alice is computed in the following ways.

Step-1: Alice sends an encrypted message (M): $E(K_2, M)$

Step-2: Darth intercepts the encrypted message and decrypts it to recover M

Step-3: Darth sends information to Bob by $E(k_1,\ M)$ or $E(K_1, M')$, where M' is any message. `Case 1:` Darth wants to eavesdrop on the communication without altering it. In the second case, Darth wants to modify the message going to Bob. The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signature and public key certificates and newly designed M.S.H. Biswas Cryptosystem.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Description of research methodology

My research methodology requires gathering relevant data from applied cryptographic article and assembling them in order to analyze the mathematical concepts applied in cryptography and arrive at more complete understanding in order to construct a new cryptosystem which will be able to solve all the problem formulated in problem statement from Michael O. Rabin cryptosystem. The problem that was formulated by me in chapter one required to study a lot of cryptographic articles related to Michael O. Rabin cryptosystem. Because, I proposed to solve all of the problem of Michael O Rabin Cryptosystem and that's why I needed to inquire about whether the formulated problem had already been solved by other researcher. It was the requirement of my research activities which was if the problem had already solved by other researcher, I had to choose another topic. I had studied more than 65 articles related to Michael O. Rabin Cryptosystem, but none of them solved the similar quadratic residue identification problem from that my confidence level grew and I stacked to it that I need to develop a new cryptosystem which would be able to solve similar quadratic residue identification problem in Michael O. Rabin cryptosystem. I hope to shed light on the following questions through my research. What could be convenient solution for identifying similar quadratic residue generated from different input? To solve the issues, I had to prototype a mathematical model for several times due to see what the solution fit for it. How was I able to solve the problem? It was great history behind my research. I started with zero knowledge protocol that was my first preference to develop a new zero knowledge protocol from existing one. I had been studying zero knowledge protocol for 5 months. But I did not find any suitable problem because it was well defined protocol and that was used in Block chain technology. One day, I was reading an elliptic curve cryptography in Wikipedia where an author mentioned that the there was no solution to identify similar quadratic residue generated from different input in Michael O. Rabin Cryptosystem. Seeing that I simultaneously changed my research topic and I had been studying Rabin cryptosystem for 18 days. I simulated a mathematical experiment by hand and I was continuing prototyping to solve that problem. I was able to solve the problem within 18 days. How did I ensure that my solution is correct? It was simple because mathematically it showed correct result in all the time. I tested by giving different input and provided real output what I expected. I had written a review article and submitted to IJSER. It was a great news for me that my research article was accepted by IJSER and it was published on June 2019 over there. But, the proposed mathematical model could not authenticate the actual sender because it was a just cipher which was unable to fulfil the requirements of cryptosystem. I studied the Rabin signature Scheme and other researcher's outcome about the Rabin signature scheme. I observed that several researcher solved the forgery attack on Rabin signature in different ways. I applied my mathematical intelligence in order to add authentication facility to update my newly developed cipher article

namely “A mathematical model for ascertaining same ciphertext generated from different plaintext in Michael O. Rabin Cryptosystem”. I had successfully implemented authentication system in October 2019. I submitted my review article namely “M.S.H. Biswas crypto-intensive techniques” to same journal for publication and that was also published on October 15, 2019 in IJSER. It was a hybrid cryptosystem which comprised 4 types key: public key, private key, shared secret key, and pre-negotiated key. I did not give mathematical proof for that because of not giving opportunity to proofreading of my article. I submitted updated version but even after I did not get any response from IJSER. I applied mathematical problem solving skills which was exploratory research techniques on an unexamined issues and I also used descriptive research type for research documentation that is called thesis. I used two type data collection instruments which were as follows:

Surveys:

I used internet based surveys and questionnaire based surveys using laptop and tab for data collection. This is a quantitative and descriptive data collection approach. A number of literature review selecting sources were considered. I had selected literature that was closely related to the research objective. I used Google search engine as a primary data collection source. I specially concentrated on scholarly article, cross reference article and other scientific articles. I downloaded literature from different sources such as Science Direct, IEEE, research gate, MDPI, Springer, Google scholarly article. I also used different social media for clarification of particular problem. The secondary data collection approach was Sci-Hub which provides free access to millions of research papers and books without regard to copyright.

Interviews:

Secondly. I had used interview based data collection technique that was qualitative and exploratory research technique. My research was exploratory research because a number of well-defined theories had been applied to solve the formulated problem of Michael O. Rabin cryptosystem. I used open questioners on Google through internet connected device. I tried to continue follow-up questions in order to keep logical sequence. I visited hundreds of website to clarify different problem. I also visited different educational media for clarifying mathematical reasoning. I sometimes experienced new issues of surface. But I also used observation technique by doing mathematical experiment. My observation technique was as follows.

Observations:

To design a new cryptosystem, I had prototyped mathematical experiment on hand many times to justify whether my method was efficient enough to fulfill a particular objective. My research was theoretical but it covers applied cryptographic research because it has real life application such as RFID chips which is greatly used in supply chain management system particularly freight monitoring system. I hope implemented cryptosystem will soon be used in RFID chips. At the final stage, when I had completed research documentation (thesis writing), it required to review in order to correction. During correction time, I took another initiatives to design a new smallest cipher where all of my beloved teachers’ names and their respective pictures will be framed as a memory. I again had succeeded to develop a new smallest cipher which was published in IJSRP on December 2019 edition namely “A systematic study

on classical cryptographic cypher in order to design a smallest cipher". All of my publications have been appended at the end of research document (List of publication). Fortunately, my research methodology was followed by agile methodology which was actually software development methodology. Because, I had intention to design a new Zero knowledge protocol, but it turned into implementation a new cryptosystem namely "M.S.H. Biswas cryptosystem" which was unexpected outcome. I think research is one of the most precious thing because it helps see the world in different window. I also think research is the only way to be a scholar. By doing this research, I have gained research experience and publication skill. My writing skills have greatly enhanced while writing this research document. I understood difference between review article, research article and research documentation. The main purpose to do research in cryptography is that I would like to achieve PhD in applied cryptography and I want to get involved in teaching profession. I would like to make a scientific carrier in computer science. It seems to me that research has great impact on human nervous system. The research is an antidote of depression. I experienced different scientific mathematical application, scientific writing method and robust sentence structure from there I influenced to achieve good communicative skills in English and that is why I am going to get admitted to MA in TESOL at Northsouth University.

CHAPTER 4

RESULTS & DISCUSION

4.1 M.S.H. Biswas cryptosystem

In this research activities, I have designed a new public key cryptosystem according to my name which was published and appended at end of this manuscript (List of publication) which can effectively encrypt and decrypt furthermore receiver can authenticate sender using signature algorithm based on Diffie – Hellman key exchange protocol, concept of square modular arithmetic from Michael O. Rabin Cryptosystem, Floor function and absolute value function. Presumably let an entity A wants communicate information to other entity B. The both entities A and B should have some confidentiality. Two entities communicate each other over insecure channel where espionage can detect the communication and reveal the sensitive information that is why an efficient technique is necessary to ensure secure communication over digital medium between two parties. They need a secret key for encoding message in order to preserve message confidentiality and ensure security. The Diffie-Hellman key exchange protocol can be used to solve these phenomenon. The both entities A and B create a shared secret key using aforesaid key exchange protocol and then both of them use same key is generated from Diffie-Hellman key exchange protocol. A encrypts secret information with a secret key so that unauthorized entity cannot presume and disclose real information. A encrypts information and chooses an equivalent residuum to generate signature by solving equation $m(m+g) \equiv (f * r * u)$ modulo k or $r(r+g) \equiv (f * r * u)$ modulo k , where r is quadratic residue modulo k, g is generator of elliptic curve, f is floor value of quadratic quotient modulus K and u (undefined random number) is selected arbitrarily to justify truthiness of equation. A sends only 4-tuple signature (f, r, u, r_e) to receiver B in case-1 and another case-2 require to send both ciphertext and signature. The entity B verifies the signature by checking truthiness of equation $r_e \equiv (f * r * u)$ modulo k or $r_e \equiv (n * r * u)\ modulo\ k$. B opens message by $\left|\sqrt{f * k + r}\right|$ if and only if aforesaid equation is true, otherwise it rejects.

Key Generation Algorithm:

$$
\begin{aligned}
K &= (Y_b)^{xa} \bmod N \\
&= (\alpha^{xb} \bmod N)^{Xa} \bmod N \\
&= (\alpha^{xb})^{Xa} \bmod N \\
&= \alpha^{xb\ Xa} \bmod N \\
&= (\alpha^{Xa})^{xb} \bmod N \\
&= (\alpha^{xa} \bmod N)^{Xb} \bmod N \\
&= (Y_a)^{xb} \bmod N
\end{aligned}
$$

https://doi.org/10.29322/ijsrp.29.12.2019

Encipher Algorithm:

To encrypt a message m, we need to computes f = $\left\lfloor \frac{m^2}{k} \right\rfloor$ *and* r = $m^2 \bmod k$, c = (f, r), where f = floor value, r = residuum, hence c = pairwise ciphertext. Ciphertexts are sometimes called hash value and denoted by h(m).

Signcryption Algorithm:

The signcryption algorithm is combination of signature generation and signature verification algorithm. To sign a message, signer S try to find the solution of the equation either $m(m+g) \equiv c * u \bmod k \Rightarrow m(m+g) \equiv (f * r * u) \bmod k$. or $r(r+g) \equiv c * u \bmod k \Rightarrow r(r+g) \equiv (f * r * u) \bmod k$. The truthiness of equation gives four tuple signature (f, r, u, r_e), where $r_e \equiv m(m+g) \bmod k$, r_e = Equivalent residuum. The verifier V verify the signatory by calculating the same equation $r_e \equiv (f * r * u) \bmod k$. Notice, verifier is actually intended receiver who open message depending on truthiness of aforesaid equation. The opening process is as follows.

Decryption Algorithm:

The verifier opens message by $\left| \sqrt{f * k + r} \right|$

4.1.1 Mathematical proof of M.S.H. Biswas Cryptosystem

Assuming that Alice wants to send a secret information for example, A=65 to Bob using valid signature. She first hashes the secret message by m ↦ m^2 modulo shared secret key and floor value of $\left\lfloor \frac{65^2}{40} \right\rfloor$. She sends together signature and hashed message with to Bob. Bob reveals message after verifying the signature of sender. The entire process is as follows.

Key generation procedure:

Table 4.1: Key Generation protocol structure

Alice (Sender)		Eve (Eavesdropper)		Bob(Receiver)	
Known	Unknown	Known	Unknown	Known	Unknown
E=113					
g=5					
Private key P=7	Q=11		7, 11	Private key Q=11	P=7
A= 5^7 mod 113				B= 5^{11} mod 113 = 34	
A=34^7mod 113 K_s = 40	34		42	B= 42^{11} mod 113 K_s = 40	

Note: g=generator, E=elliptic curve area,* K_s*= shared secret key*

Base step for cipher algorithm:

The square is a number multiplied by itself. The squaring function can transform an integer number into a natural number. The rules of mathematics imply that transformation of squared number to squared free number require square root function which is actually inverse function of square number. In mathematics, an inverse function or anti-function is a function that reverse another function: if the function f applied to an input x gives a result of y, then applying its inverse function g to y gives the result x and vice versa, i.e., f(x) = y iff g(y) = x. The division is inverse of multiplication according to basic mathematical rules. The truthiness of encipher method and decipher method for initial value is as follows. Let message (m) = 1, $m \mapsto m^2$

$$\text{Cypher text } (c) = (f, r) = \begin{cases} \text{Floor value } (f) = \left\lfloor \frac{1^2}{40} \right\rfloor = 0 \\ \text{Residuum } (r) = 1^2 \bmod 40 = 1 \end{cases} \quad \text{.....Equ.(1)}$$

$$\text{Plaintext} = \text{Decryption} = \text{d} = \left|\sqrt{f * k + r}\right| \quad \text{.....Equ.(2)}$$

$$= \left|\sqrt{0 * 40 + 1}\right|$$

$$= \left|\sqrt{1}\right| = 1 \text{ (proved).}$$

As base case is true, depending on it the next step can be proceeded.

Induction Step for Cipher algorithm:

If a decimal number is divided by another one, the quotient and remainder are generated as per basic mathematical rule. In other perspective, quotient can be counted by floor function and remainder can be counted by modular arithmetic.

A general division arithmetic for example- (divider)40 $\Big|$ 105(quotient)
65^2=4225(divident)
−40
225
−200
25(remainder)

The keyword is divider which often acts in this cryptosystem as a division arithmetic at time as modular arithmetic where divider is indicated as a modulus. Since division is inverse of multiplication according to basic mathematics, for that reason, to retrieve the message quotient will have to be multiplied by the divider (keyword) and remainder will also have to be multiplied by the divider and then both will have to be added, because a natural number is divided into two parts. But in this cryptosystem, the remainder does not need to multiply with divider when message is retrieved because of modular arithmetic readily calculate residue which is equivalent to number after decimal

point × modulus. Therefore, for the reconstruction of the message, at first three distinct number will have to be recombined as reverse to sender actions which is as follows.

$$floor\ value * keyword + residue$$

This function construct a new number which is actually squared number. As quotient and residue are derived from squared number, square root function must be used to make it square free like $\sqrt{floor\ value * keyword + residue}$. The result derived from it will be either positive or negative value but natural number is to be counted only using absolute value function like $\left|\sqrt{floor\ value * keyword + residue}\right|$. This computation must result in original message according to mathematical logic. Suppose for $m = n\ and\ k = n$, proposed cipher technique is true. Let us see the truthiness of cipher technique is as follows.

$$\text{Quotient}(q) = \lfloor n^2 \div n \rfloor = n,\ \text{Residuum (r)} = n^2 \bmod \text{n} = 0$$

$$\text{Cypher text (c)} = (q, r) = (\text{n}, 0)$$

$$\text{Decryption} = \text{d} = \left|\sqrt{q * k + r}\right|$$
$$= \left|\sqrt{n * n + o}\right|$$
$$= \left|\sqrt{n^2}\right| = \text{n (Proved)}$$

Since proposed cipher technique results in n terms correctly, the mathematical induction for proposed cipher technique is correct.

`Base step for Syncryption Algorithm:`

It is necessary, both quotient and residuum must be natural number that is greater than zero in order to generate signature for M.S.H. Biswas cryptosystem. The division arithmetic means that distribute integer number among divider and remaining left as a remainder because it cannot be distributed as a round number. When an even number is divided by an odd number likewise an odd number is divided by an even number, the calculator results in rational number which contains two parts: left-hand side is an integral number and right hand side fractions part. To calculate number after decimal point, the modular arithmetic is required which results in integer number.

`Induction step for Syncryption:`

The proposed syncryption algorithm works better depending on two proposition. The signature can be generated and verified by two significant ways: One of them is described in case-1 and other one is illustrated in case-2.

Case-1: Signature generation & verification

- Signature can be generated depending on following proposition.

(1) $\begin{cases} \text{Floor value } (f) = \lfloor m^2 \div k \rfloor & iff\ m^2 \geq k \quad \& \ m \not\equiv 0 \\ \text{Residuum } (r) = m^2 \bmod k & iff\ m \not\equiv 0 \quad \& \ m^2 \not\equiv k \end{cases}$

According to assertion (1), *Equ.(3)* must be true to generate signature.

$$\begin{aligned} m(m+g) &\equiv \{h(m) * u\} \bmod k \\ &\equiv (c * u) \bmod k \\ &\equiv (f * r * u) \bmod k \quad \ldots\ldots\ldots\ldots \textit{Equ.(3)} \end{aligned}$$

To make signature is more intractable, *Equ.(3)* can also be written as

$r(r+g) \equiv (f * r * u) \bmod k$ .Now let us see *Equ.(3)* has to be true satisfying proposition (1). For instance, message (65) plugging in *Equ.(3)*

$$\begin{aligned} 65(65+5) &\equiv (105 * 25 * 14) \bmod 40 \\ \therefore 30 &\equiv 30 \ (\text{modulo } 40) \end{aligned}$$

Since equivalent residue r_e= 30. Depending on it sender generates 4-tuple signature (105, 25, 14, and 30) based on *Equ.(1,2 and 3)* and sends it to receiver. Receiver is the verifier who verify signature by calculating *Equ.(4)* is as follows.

$$\begin{aligned} r_e &\equiv (f * r * u) \bmod k \ldots\ldots\ldots\ldots\ldots\ldots \textit{Equ.(4)} \\ &\equiv (105 * 25 * 14) \bmod 40 \\ &\equiv 30 \ (mod\ 40) \text{ [Verified]} \end{aligned}$$

Verifier decrypts message by depending on truthiness of above equation. If any value of four tuple signature is altered during transmission, the aforesaid equation becomes fails and verifier reject message. Otherwise, signature is accepted by verifier and he or she will open the message by decipher method *Equ.(2)* is as follows.

$$\begin{aligned} D &= \left|\sqrt{q * k + r}\right| \\ &= \left|\sqrt{105 * 40 + 25}\right| \\ &= \left|\sqrt{4225}\right| = 65 = A \text{ (proved).} \end{aligned}$$

As it is shown that signature generation and verification according to proposition (1) and *Equ.(3,4)* is true, for this reason, mathematical induction is proved for case-1.

Case-2: Signature generation & verification

- Signature can be generated depending on following proposition.

(2) $\begin{cases} \text{ceiling value } (n) = \lceil m^2 \div k \rceil \ \ iff\ m^2 < k & \& \ m \not\equiv 0 \\ \text{Residuum } (r) = \ m^2 \bmod k \quad iff\ m \not\equiv 0 & \& \ m^2 \not\equiv k \end{cases}$

According to assertion (2), *Equ.(5)* must be true to generate signature.

$$\begin{aligned} m(m+g) &\equiv \{h(m) * u\} \bmod k \\ &\equiv (c * u) \bmod k \\ &\equiv (n * r * u) \bmod k \quad \text{.....Equ.(5)} \end{aligned}$$

To make signature more intractable, *Equ.(5)* can also be written as

$r(r+g) \equiv (n * r * u) \bmod k$ .Now let us see *Equ.(5)* has to be true satisfying proposition (2). For instance, message (1) plugging in *Equ.(5)*

$$\begin{aligned} 1(1+5) &\equiv (1 * 1 * 6) \bmod 40 \\ \therefore 6 &\equiv 6 \ (\text{modulo } 40) \end{aligned}$$

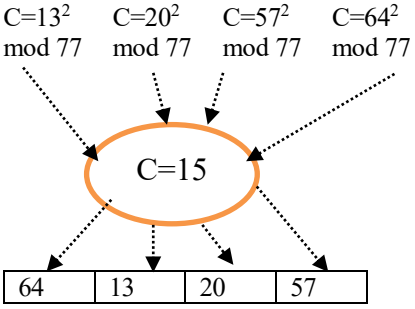
So equivalent residue r_e= 6. Sender generates 4-tuple signature (1, 1, 6 and 6) based on *Equ.(1,2 and 5)*. In this case-2, Sender has to be sent four tuple signature together with ciphertext to receiver. Because receiver can verify signatory of intended sender but it cannot open message from signature only. Receiver is the verifier who verify signature by calculating following equation.

$$\begin{aligned} r_e &\equiv (q * r * u) \bmod k \quad \text{.....Equ.(6)} \\ &\equiv (1 * 1 * 6) \ mod\ 40 \\ &\equiv 6 \ (mod\ 40) \text{ [Verified]} \end{aligned}$$

Verifier decrypts message by depending on truthiness of *Equ.(6)*. If any value of four tuple signature is altered during transmission, the aforesaid *Equ.(6)* becomes false and verifier reject message. Otherwise, signature is accepted by verifier and open message by decrypting ciphertext in similar fashion *(Equ.(2))*. As it is shown that signature generation and verification by *Equ.(5, 6)* satisfying proposition (2) is true, for this reason, mathematical induction is proved for case-2.

4.1.2 Comparison of Michael O. Rabin and M.S.H. Biswas Cryptosystem

Table 4.2: The comparison between two cryptosystems.

Michael O. Rabin Cryptosystem	M.S.H. Biswas Cryptosystem
1. Ciphertext is a quadratic residue. 2. Decryption generates 4-tuple 3. It uses asymmetric key 4. This is a asymmetric cryptography 5. It does not offer simultaneous communication between two entities. 6. It facilitates one party active other party passive. 7. It is vulnerable against chosen ciphertext and plaintext attack. 8. Michael O. Rabin's Encryption and decryption system cannot identify same ciphertext generated from different plaintext. For example,  9. C = 15 which against what input that is encryption failure and to decrypt C = 15 result in same 4-tuple that is decryption failure. 10. One party key issuer other party message sender. Both party cannot communicate simultaneously because key issuer wait for other party's message. Secret key possesses only one party. 11. Advantage of Michael O. Rabin Signature:	1. Ciphertex is a pair of integer. 2. Decryption result in single plaintext. 3. It uses shared secret key publicly. 4. This is public key cryptosystem. 5. It offers simultaneous communication between two entities. 6. It facilitates the both entities active. 7. It is strong against man in the middle attack, brute-force attack, modulus exponential attack, chosen ciphertext and plaintext attack. 8. It is strong due to having ability to distinguish same Ciphertext uniquely generated from different plaintext. 9. Proposed technique can identify same ciphertext against different plain text. 10. proposed cypher can efficiently identify same residues separately generated from distinct plaintext using quotient-residuum technique is as follows: Plaintext m = 13, Residuum=13^2mod 77 Quotient= $\left\lfloor \frac{13^2}{77} \right\rfloor$, Corresponding encrypted text C = (2,15) Plaintext m = 20, Residuum=20^2 mod 77=15, Quotient= $\left\lfloor \frac{20^2}{77} \right\rfloor$=5, Corresponding encrypted text C = (5,15) Plaintext m = 57, Residuum=57^2 mod 77=15, Quotient=$\left\lfloor \frac{57^2}{77} \right\rfloor$=42, Corresponding encrypted text

The signature actually contains several interesting feature are ○ The signature is possible using Every pair of primes. ○ Different signatures of the same Documents are different. 12. The verification needs only two multiplications and therefore it is fast enough to be used in authentication protocol 12. Disadvantage Michael O. Rabin Signature: It is vulnerable to forgery attacks. It is relatively easy to compute $S^2 \, mod \, N$ and choose any message m' after that compute multiplicative inverse of m' (hash value of m), compute $U' = (S^2 * m'^{-1})$ mod N and forge the signature as (m'^{-1}, U', s) without knowing the factorization of N.	C = (42,15) Plaintext m = 64, Residuum=64^2 mod 77=15, Quotient=$\left\lfloor \frac{64^2}{77} \right\rfloor$=53, Corresponding encrypted text C = (53,15) 11. The proposed crypto intensive technique can uniquely identify each cipher text against plaintext 12. It is unforgeable in forgery attack while Rabin signature is forgeable in forgery attack. 13. Advantage of M.S.H. Biswas Signature: The signature is generated by computing the congruence equation $m(m + g) \equiv c * u \bmod k$. It require less time complexity compare to Michael O. Rabin public key signature scheme. 14. It is unforgeable against forgery attack

CHAPTER 5

CONCLUSIONS

1.1 Conclusion

The proposed M.S.H. Biswas cryptosystem is efficient for solving identification of problem of similar quadratic residue generated from different plaintext in Michael O. Rabin cryptosystem on the one hand. On the other hand, the signature algorithm is capable to handle forgery attack, chosen plaintext attack, Brute force attack, and man-in-the middle attack. It helps removing four to one mapping signature and one to four mapping decryption. Identification each ciphertext separately was the first objective because modular arithmetic can generate same cyphertext from different plaintext. The proposed mathematical model can efficiently identify each ciphertext separately generated form modular reduction arithmetic. To verify sender and validate message through signature verification system was 2nd objective where both authentication and integrity elements have been successfully deployed to implement signature scheme. Proposed key generation technique is derived from Diffie – Hellman key-exchange protocol but there was a security vulnerability in symmetric key generation stage (man in the middle attack), because it could not authenticate the participants. The proposed cryptosystem not only provided solution of similar quadratic residue identification problem but it also ensure security and confidentiality by syncription algorithm..

1.2 Research Contributions

In this research activities, a new public key cryptosystem has been designed by removing barrier of similar quadratic residue identification problem in Michael O. Rabin cryptosystem. It consists of Key generation algorithm, Encryption algorithm, Decryption algorithm, Signature generation algorithm and Signature verification algorithm,

1.3 Future Work

I would like to leave encryption scheme for future cryptographic reader to make concrete ciphertext which can uniquely identify similar quadratic residue separately generated from different input.

REFERENCES

Alex, A., Wool, A. & Yossef, O, (Tel-Aviv and Columbia University), (2014). A Secure Supply-Chain RFID System that respects your privacy, In: Published *by the IEEE CS,* 1536-1268/14/IEE

Awad, Y.Kassar, A.N. EI & Kadri, T.(2018). Rabin public-key cryptosystem in the domain of Gaussian Integers, *In: International conference on computer and application (ICCA).*

Apostol, T.M.(1976). Introduction to analytic number theory, Springer, new York, and *wikipedia has good description about Direclet theorem on arithmetic progression.*

Bezout , E(1779), Theory generate a statement in algebraic geometry. Paris, France: Phd, Pierres. Weisstein. Eric W, Bezout's Identity, *Mathworld.*

Bellare, M. & Neven, G. (2006) Multi-Signatures in the Plain Public-Key Modeland a General Forking Lemma, CCS, Alexandria, Virginia, USA, ACM 1-59593-518-5/06/0010

Berzati & Goubin L.(2008). Perturbing RSA public keys: An improved attack, In E.Oswald, P.Rohatgi (eds.): Cryptographic Hardware & Embedded *System (CHES), Lecture notes in computer science* vol.5154, springer and pp.380-395

Berzati, A., Canovas-Dumas, C. &. Goubin, L(2009) Fault attacks on RSA public Keys: Left-To-Right implementations are also vulnerable. *In: M. Fischlin (ed): CT- RSA, Lecture notes. vol.5473, Springer, pp.414-428*

Bhatt, M., Shweta S. & Deshmukh, M. (2018).Deterministic Rabin Cryptosystem, *In: 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT*), Research gate publication no.325330795

Bernstein, D. J. (2008). RSA and Rabin-William signatures: The state of the art", *In: EUROCRYPT, Proceeding of the theory and applications of cryptographic techniques 27th annual international conference on advances in cryptology pages. 70-87, ISBN: 3-540-78966-9, 978-3-540-78966-6*

Bleichenbacher, D.(2004). Compressing Rabin Signatures, *In: T. Okamo to (Ed.): CT- RSA, LNCS 2964, pp.126-128, Springer- Verlag Berlin Heidelberg, Bell labs-Lucent Technologies.*

Chaoyang Li, Xiangjun xin and Xiaolin Hua,(2017). An efficient ID-based Rabin signature without pairings, *In: International Journal of Multimedia and Ubiquitous Engineering* Vol.12, No.3 (2017), pp.75-80, doi:10.14257/jimue.2017.12.3.08

Chandrakar, P. & Hari O, (2017). An efficient two factor remote user Authentication and session key agreement scheme using Rabin cryptosystem, doi: 10.1007/s13369-2709-6

Chakraborty, R.,Biswas, S. & Mandal, JK, (2014). Modified Rabin Cryptosystem through Advanced Key Distribution System, *In: Journal of Computer Engineering* (IOSR-JCE) e-ISSN: 2278-0661, P-ISSN: 2278-8727 Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP. 01-07, www.iosrjournals.org

Choi, D. Jun, B. Lee, J.& Subong L.,(2018).Arithmetic of generalized Dedekind sums and their modularity[Online]: doi: 10.1515/math-2018-0082

Drane, T., Cheung, W. & Constantinides, G. (2012). Correctly Rounded Constant Integer Division Via Multiply-add, *In: The IEEE International Symposium on Circuits and Systems, Conference Paper,* doi: 10.1109/ISCAS. 2012.6271461

Dong, X. Han S. & Yun (2017). A modifications of the Rabin cryptosystem based on cubic residues, *In : Communications, information management and network security (CIMNS), ISBN*: 978-1-60595-498-*1*

Editor, Dailystar (2016).Bangladesh Bank reserve hacking *In: https://www.thedailystar.net/tags/Bangladesh bank-hacking*

Elia, M, Piva, M. & Schipani, D.(2013). The Rabin cryptosystem revisited. arXiv:1108.5935v3 [math.NT], Mathematics Subject Classification (2010):94A60, 11T71, 14G50

Elia, M. Piva, M. & Schipani, D.(2011). Rabin cryptosystem revisited Elia, M. & Schipani, D.(2010). On the Rabin signature, *In: Journal of Discrete Mathematical Science and Cryptography 16(6).*

Elia, M. Piva, M. & Schipani, D.(2013). Rabin cryptosystem revisited, *In: Mathematics subject classification (2010):94A60, 11T71, 14G50, University of Zurich, Switzerland,*

Frohlich, M,J &Taylor (1994). Algebraic Number Theory, Cambridge Univ. Press. Gauss, C. F. Arthur, T. Clark, A. (1965). Disquisitiones Arithmeticae, *Yale University Press, ISBN:* 0-300-09473-6

Grosswald, E., (2009). Topics from the Theory of Numbers, Birkhauser, Basel

Gani, H. (2019). A mathematical analysis of RSA and Rabin Cryptosystem, *In: Researchgate publication no. 332834881(2019)*

Hasim,, H. R.(2014). H-Rabin Cryptosystem, *In: Journal of Mathematics and Statistics*. doi: 10.3844/jmssp.2014.304.308, *Researchgate publication:264286919*

Hardy, G. H., E.M. Wright (1971), An Introduction to the Number theories, Oxford: *Clarendon Press,*

Hardy, G.H. & Wright, E.M (1980). An introduction to the Theory (5th ed). Oxford: *Oxford University Press, ISBN:* 978-0-19-853171-5

Ireland, K., M. & Rosen,(1998.). A Classical Introduction to Modern Number Theory, New York, Springer

Jones, G. A. & Jones, J.M.(*1998*).The Legendre symbol, 7.3 in Elementary Number Theory Berlin, Springer-*Verlag,* pp.123-129,

Jaweria, Usmani, Prakash, J. (2017). A secure gateway discovery protocol using Rabin signature scheme in MANET, *In: International Journal on Communications Antenna and Propagation* 7(5):439 doi: 10.15866/irecap.v7i5.12581

Kaminaga, M. Yoshikawa, H., Shikoda, A. & Suzuki, T. (2016) Member IEEE, Crashing Modulus Attack on Modular Squaring for Rabin Cryptosystem. doi:10.1109/TDSC.2016.2602352, IEEE

Klimov, N.I (2001), Mobius function, *In* Hazewinkel, Michael Edward, Encyclopedia of Mathematics, Springer Science+ Business Media B.V./ *Kluwer Academic Publishers, ISBN:* 978-1-55608-010-4

Karen, M. Strom,(2012). ASCII-Sticks and Stones, an alphabetic book for the 21st century.*Publisher: Polytropos Press*, *ISBN:* 9780988378520

Knuth G. & Patashnik,(1988). Concrete Mathematics: A foundation for computer science.(2nd ed.), ISBN-10:0201558025

Katz & Victor J.(1998), a History of mathematics, an Introduction (2nd edition).*Addison Wesley Longman, ISBN: 978- 0-321-01618-8*

Lemmermeyer, F.,(2000). Reciprocity Laws, New York, Springer.

Manuel, Bronstein, et.al., eds.(2006). Solving Polynomials Equations: Foundations, Algorithms and applications. Springer, *ISBN:* 978-3-540-27357-8

Menzes A., P.van Oorschot and S. Vanstone (1997). Michael O. Rabin Cryptosystem, *In: Handbook of Applied Cryptography*

Mahad, Z. & Ariffin, M. R. K.(2015). A new efficient method to overcome Rabin cryptosystem decryption failure Problem, *In: International Journal of Cryptology Research 5(1):11-20(2015)*

Peter, H.(2013) .The distribution of weighted sums of the Liouville function and Polya's Conjecture, In: *Journal of Number Theory,* 133(2):545-582. Arxiv: 1108.1524, doi:10.1016/j.jnt

Pieprzyk, J. Hardjono, T. & Seberry, J.(2003) Fundamentals of Computer Security, New York: springer.

Rabin, Michael. O. J.F. Traub, eiditor. (1976) Probabilistic algorithm, algorithm and complexity, recent results and new directions, *academic press, inc.* New York, San Francisco, pp.21-40

Rabin,, Michael O. (1979). Digitized signatures and public key functions as intractable as factorization, *Technical report MIT-LCS-TR-212, MIT laboratory for computer science.*

Rademacher, H.. E. Grosswald, (1972).Dedekind Sums, MAA, New York,

Roger, N. & Michael, S.,(1978). Using encryption for authentication in large networks of computers, Communication of the ACM. 21(12):993-999, doi: 10.1145/359657.359659

Saxl, G., Ferdik, M., Fischer,M., Maderboeck, M. and Ussmueller,T.(2019). Article UHF RFID prototyping Platform for ISO 29167, Decryption based on an SDR, www.mdpi.com/journal/sensors, *Sensors,*19.2220: *doi:*10.3390/s19102220

Stallings, W .(2016). Cryptography and Network security Principles and Practices.(6th ed.) ,*India, Pearson Press. ISBN:* 978-93-325-1877-3.

Sattar, I., Raheem, A. Hamad, M. H.(2015). Design and implement Rabin crypto code as Guider for Stego-system, Al Mustansiriyah University.

Srivastava, A. K. & Mathur, A.(2013). The Rabin Cryptosystem & analysis in measure of Chinese Remainder Theorem, *In: International Journal of Scientific and Research Publications,* Volume 3, Issues 6, June 2013, ISSN: 2250-3153

Sidorov, E.& Kandex LLC(2015). Breaking the Rabin-Williams digital signature system implementation in Crypto++ library*, In: Journal of Cryptology, iacr.org,*

Stallings, W.(2016). Cryptography and Network Security Principles and Practices, 6th Edition. ISBN: 978-93-325-1877-3, India: *Pearson press.*

Takagi, T. & S. Naito, (1997). An extension of Rabin Cryptosystem to Eisenstein and Gauss Fields, IEICE Trans. Fundamentals, Vol. E80-A.

Varil, A.,(2014) Dirichlet's Theorem on arithmetic Progressions, Harvard University, Cambridge, MA 02138

Wikipedia has good description about Group Isomorphism.

Williams, H.C., (1998). A modification of the RSA public-key encryption procedure*,* IEEE $Trans, on\ inform, Th. IT$- 26(6), pp.726-729

Waite, W.M. ((1987).Needham, R. M., Schroeder, Authentication revisited, ACM *SIGOPS Operating System Review,* 21(1):7. doi:10.1145/24592.24593

Williams, H.C.(1980). A modification of the RSA public key encryption procedure, *IEEE Trans. On Information theory, IT-26(6), pp.726-729*

APPENDIX A

Table A.1: ASCII values

Letter	ASCII	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

APPENDIX B

Table B.1: Infinitely many prime formation

Arithmetic progression	First 10 prime number counting
$2n + 1$	$3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$
$4n + 1$	$5, 13, 17, 29, 37, 41, 53, 61, 73, 89, \ldots$
$4n + 3$	$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, \ldots$
$6n + 1$	$7, 13, 19, 31, 37, 43, 61, 67, 73, 79, \ldots$
$6n + 5$	$5, 11, 17, 23, 29, 41, 47, 53, 59, 71, \ldots$
$8n + 1$	$17, 41, 73, 89, 97, 113, 137, 193, 233, 241, \ldots$
$8n + 3$	$3, 11, 19, 43, 59, 67, 83, 107, 131, 139, \ldots$
$8n + 5$	$5, 13, 29, 37, 53, 61, 101, 109, 149, 157, \ldots$
$8n + 7$	$7, 23, 31, 47, 71, 79, 103, 127, 151, 167, \ldots$
$10n + 1$	$11, 31, 41, 61, 71, 101, 131, 151, 181, 191, \ldots$
$10n + 3$	$3, 13, 23, 43, 53, 73, 83, 103, 113, 163, \ldots$
$10n + 7$	$7, 17, 37, 47, 67, 97, 107, 127, 137, 157, \ldots$
$10n + 9$	$19, 29, 59, 79, 89, 109, 139, 149, 179, 199, \ldots$
$12n + 1$	$13, 37, 61, 73, 97, 109, 157, 181, 193, 229, \ldots$
$12n + 5$	$5, 17, 29, 41, 53, 89, 101, 113, 137, 149, \ldots$
$12n + 7$	$7, 19, 31, 43, 67, 79, 103, 127, 139, 151, \ldots$
$12n + 11$	$11, 23, 47, 59, 71, 83, 107, 131, 167, 179, \ldots$

APPENDIX C

Table C.1: The generator of group $G_1 = \{3, 5\}$ under mod 7

First subgroup of elements	g^{μ} *mod 7*	g^1	g^2	g^3	g^4	g^5	g^6	Comments
	1	1	1	1	1	1	1	1st row-column unique
	2	2	4	1	2	4	1	×
	3	3	2	6	4	5	1	Generator
	4	4	2	1	4	2	1	×
	5	5	4	6	2	3	1	Generator
	6	6	1	6	1	6	1	×

Table C.2: The generator of group $G_2 = \{2, 6, 7, 8\}$ under modulo 11

g^{μ} *(11)*	g^1	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}	*Comments*
1	1	1	1	1	1	1	1	1	1	1	1st row-col same
2	2	4	8	5	10	9	7	3	6	1	Generator
3	3	9	5	4	1	3	9	5	4	1	×
4	4	5	9	3	1	4	5	9	3	1	×
5	5	3	4	9	1	5	3	4	9	1	×
6	6	3	7	9	10	5	8	4	2	1	Generator
7	7	5	2	3	10	4	6	9	8	1	Generator
8	8	9	6	4	10	3	2	5	7	1	Generator
9	9	4	3	5	1	9	4	3	5	1	×
10	10	1	10	1	10	1	10	1	10	1	×

Table C.3: The modular additive group of N=77

+	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38

+	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
19	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57
20	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
21	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
22	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
23	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
24	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
25	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
26	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
27	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
28	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
29	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67
30	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
31	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69
32	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70
33	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71
34	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72
35	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73
36	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
37	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75

https://doi.org/10.29322/ijsrp.29.12.2019

+	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57
38	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
39	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
40	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
41	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
42	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
43	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
44	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
45	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
46	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
47	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
48	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
49	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
50	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
51	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
52	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
53	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
54	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
55	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
56	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
57	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37

+	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
58	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57
59	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
60	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
61	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
62	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
63	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
64	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
65	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
66	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
67	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
68	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67
69	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
70	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69
71	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70
72	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71
73	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72
74	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73
75	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
76	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75

LIST OF PUBLICATIONS

1. **Md. Shamim Hossain Biswas*,** Dr. Md. Asraf Ali, Dr. Mostafijur Rahman, Mr. Md. Khaled Sohel, Mr. Md. Maruf Hasan, Kausik Sarkar, Abu Shamim Aminur razzaque, "A systematic study on classical cryptographic cypher in order to design a smallest cipher**",** *In :* ***International Journal of Scientific and Research Publications****,* Volume 9, Issue 12, Month 2019, ISSN 2250-3153.
   DOI: https://doi.org/10.29322/ijsrp.9.12.2019.p9662 [Cross-reference]

2. **Md Shamim Hossain Biswas**, "M.S.H. Biswas crypto-intensive techniques", *In:* ***International Journal of Scientific & Engineering Research*** Volume 10, Issue 10, (2019). ISSN 2229-5518,
   DOI: 10.14299/ijser.2019.10.01 [Cross-reference]

3. **Md Shamim Hossain Biswas**,"A mathematical model for ascertaining same ciphertext generated from distinct plaintext in Michael O. Rabin Cryptosystem", *In:* ***International Journal of Scientific & Engineering Research*** Volume 10, Issue 6 (2019). ISSN 2229-5518,
   DOI: 10.14299/ijser.2019.06.08 [Cross-reference]

4. **Md. Shamim Hossain Biswas**, "Congestion Analysis of Transmission Control protocol", In: ***International Journal of Scientific & Engineering Research.*** ISSN 2229-5518, Thesis Publication.
   DOI: https://doi.org/10.14299/ijser.thesis.2020.01 [Cross-reference]